EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Irvine Unified School District and which is May 6, 2020 to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS

By: _____ Date: May 6, 2020

Printed Name: Jeremy Loch Title/Position: SVP & General Manager, School Solutions

2. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Term. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

By: _____ Date: 5.4.24

Printed Name: E.J. Rossi Title/Position: Assistant Superintendent

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW:

Name: Shelley R. Lorren

Title/Position: Senior Sales Operations Specialist

Email Address: shelley.lorren@e-hps.com

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

IRVINE UNIFIED SCHOOL DISTRICT

and

HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS

May 6, 2020

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Irvine Unified School District (hereinafter referred to as ;'LEA") and **HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS** (hereinafter referred to as "Provider") on MAY 6, 2020. The Parties agree to the terms stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to the MySchoolBucks Master Services Agreement dated May 6, 2020 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Software solution to support the following, but not limited to: meal applications, online pre-payments, point of sale transactions, transportation, field trips, spirit wear, and Nutrition Services operations and accountability requirements.

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall, to the extent permitted by law, redirect the Third Party to request the data directly from the LEA. To the extent permitted by law, Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subcontractor.** Provider shall enter into written agreements with all Subcontractors performing functions pursuant to the Service Agreement, whereby the Subcontractors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other applicable California privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Authorized Use.** The data provided by LEA to Provider pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the

Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or when Provider is no longer under a legal, regulatory, or audit requirement to retain it. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed (i) to complete the disposition or (ii) to comply with Provider's legal, regulatory, or audit obligations. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services unrelated to Provider's Service Agreement, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standard technology practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any

other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or when Provider is no longer under a legal, regulatory, or audit requirement to retain it, and may transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition or comply with Provider's legal, regulatory, or audit obligations.

c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA or provide the Services.

d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subcontractors Bound.** Provider shall enter into written agreements whereby Subcontractors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessment of Subcontractors to determine their compliance with this Article.

h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual Provider shall provide prompt notification to LEA within a reasonable amount of time of

discovery of the incident, not exceeding seven (7) calendar days. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein, to the extent known at the time of the notice, under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information, to the extent known at the time and not prohibited by law enforcement:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what Provider has done to protect individuals whose information has been breached.
ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable State and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects industry standard practices and is consistent with federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA or required by applicable law. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for third party costs incurred to

notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA as reasonably necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1 (b), and Article II, section 3, above, other than any data that Provider may be under a legal, regulatory, or audit obligation to retain.

4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. **Designated Representatives**

The designated representative for the LEA for this Agreement is:
Name: Michelle Bennett
Title: Specialist – IT Contracts

Contact Information:
Irvine Unified School District
5050 Barranca Parkway

Irvine, CA 92602
949-936-5022
MichelleBennett@iusd.org

The designated representative for the Provider for this Agreement is:
Name: Tyson Prescott
Title: Senior Director, Software Development

Contact Information:
765 Jefferson Road, Suite 400, Rochester, NY 14623
800-724-9853
Tyson.prescott@e-hps.com

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Jeremy Loch
Title: SVP & General Manager, School Solutions

Contact Information:
765 Jefferson Road, Suite 400, Rochester, NY 14623
800-724-9853
Jeremy.loch@e-hps.com

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF ORANGE COUNTY, CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR ORANGE COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver.** No delay or omission of either party to exercise any right hereunder shall be construed as a waiver of any such right and each party reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

IRVINE UNIFIED SCHOOL DISTRICT

By: _____ Date: May 5, 2020

Printed Name: John Fogarty Title/Positon: Asst. Supt. Business Services/CFO

IUSD Board Approval: May 26, 2020 * ratification

HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS

By: _____ Date: May 6, 2020

Printed Name: Jeremy Loch Title/Positon: SVP& General Manager, School Solutions

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Software solution to support the following, but not limited to: meal applications, online pre-payments, point of sale transactions, transportation, field trips, spirit wear, and Nutrition Services operations and accountability requirements.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID number	
	Student app usernames	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data -Please specify:	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	MSB can create custom web forms designed to capture information specific to the IUSD transportation program.
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code§ 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term 'Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable California statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the MySchoolBucks Contract which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Student Data: Student Data includes any data provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subcontractor: For the purposes of this Agreement, the term "Subcontractor" means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Irvine Unified School District directs HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

Extent of Disposition Disposition shall be:	X Partial. The categories to be disposed of are as follows: Personally Identifiable Data ____ Complete: Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	X Destruction or deletion of data. ____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred. Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	X As soon as commercially practicable. ____ By (Insert Date) _____

Authorized Representative of LEA — May 5, 2020 — Date

-Jeremy Loch — May 6, 2020

Verification of Disposition of Data
By Authorized Representative of Provider — Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Irvine Unified School District and which is May 6, 2020 to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

HEARTLAND PAYMENT SYSTEMS LLC, dba HEARTLAND SCHOOL SOLUTIONS

By: _____ Date: May 6, 2020

Printed Name: Jeremy Loch Title/Position: SVP & General Manager, School Solutions

2. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Term. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW:

Name: Shelley R. Lorren

Title/Position: Senior Sales Operations Specialist

Email Address: shelley.lorren@e-hps.com

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Please reference the attached documents:

1. Heartland School Solutions Data Security and Privacy Plan
2. Heartland Mosaic Cloud Disaster Recovery Plan
3. MySchoolApps Data Security and Privacy Plan
4. MSB Privacy Policy

Heartland School Solutions Data Security and 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 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.

DISASTER RECOVERY PLAN

AUGUST 2016

Heartland

Table of Contents

Scope / Purpose

This document provides information regarding the Heartland School Solution's Mosaic Cloud Disaster Recovery Plan (DRP). A disaster recovery plan is a documented process or set of procedures to recover and protect business IT infrastructure in the event of an incident compromising the Heartland data center supporting Mosaic Cloud. The objective of a disaster recovery plan is to minimize downtime and data loss. Minimizing downtime and data loss is measured in terms of two objectives: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the maximum acceptable amount of data loss.

Objectives

Recovery Time Objective: 5 minutes

Recovery Point Objective: No data loss

Recovery Strategy

The recovery strategy includes full and incremental backups, data replication and automated failover from the primary data center to a remote DR site, provided the primary DC is still functional. Real time production data is replicated in asynchronous mode to database servers at the DR location supporting uninterrupted processing in the event of primary server failure. Key highlights:

- Full nightly database backup within retention policy
- Transaction log backup performed every 30 minutes within retention policy
- Primary DC Database server redundancy (synchronous mirroring on the Availability Group)
- Secondary DC Database server redundancy (asynchronous mirroring on the Availability Group)
- High availability SAN
- Web/Application server redundancy using a load balancer network device
- Virtual server re-provisioning with a 24hr recovery window
- 24 X 7 NOC monitoring, alerts, on call Operations activation, full ticket tracking
- Major Incident Response Process

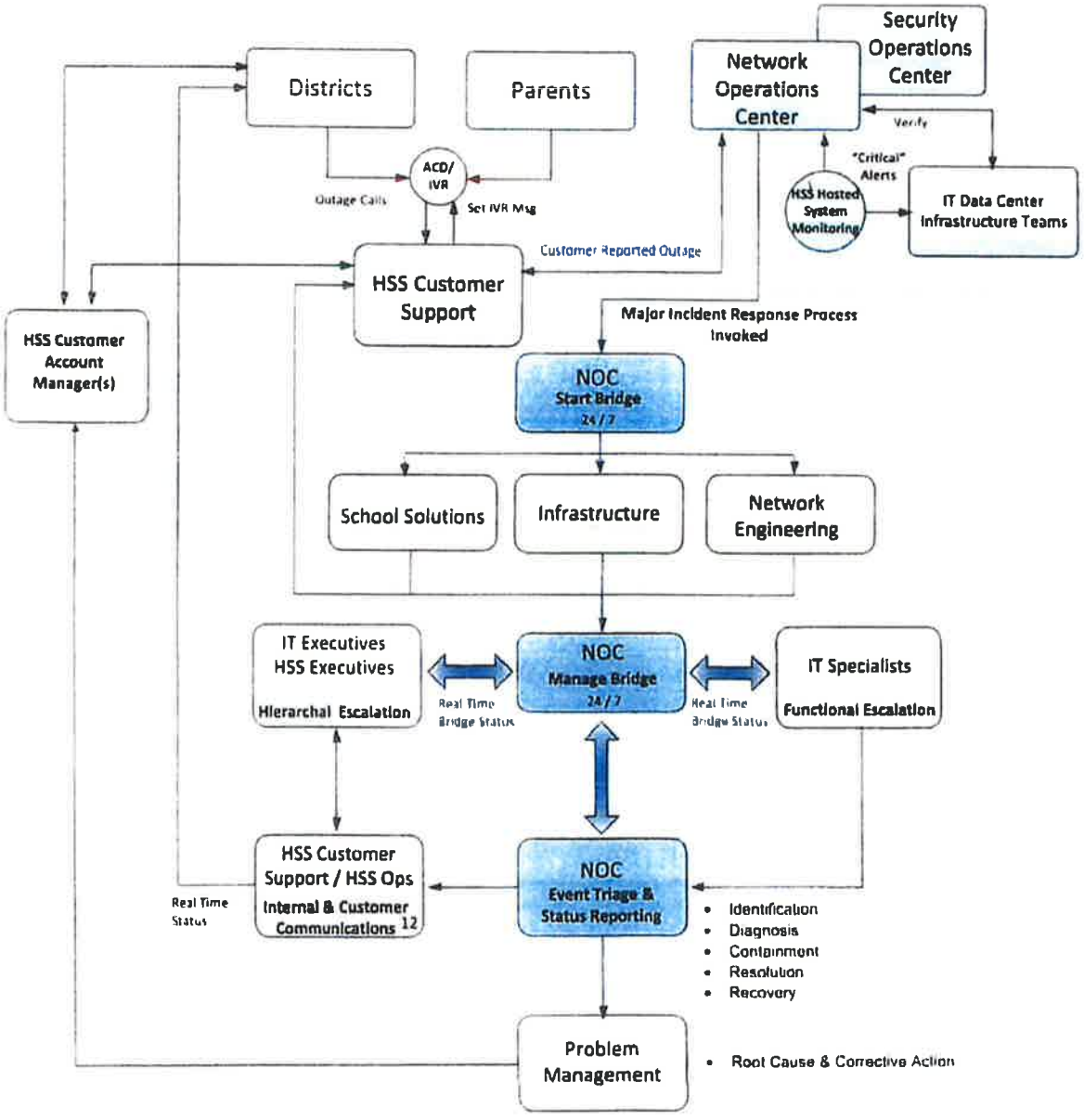
In the event of a specific web, application or database server issue, failover is automatic and instantaneous. If an entire layer is rendered unusable, failover of the entire layer at our remote secondary data center is instantaneous. Failover in the event of catastrophic event rendering our primary data center unusable, a Major Incident Response Team will ensure recovery in our secondary data center. System performance, in any DR recovery scenario, will be transparent to our customers.

Heartland

Major Incident Response Process

In the event of any major incident affecting Heartland School Solutions Mosaic Cloud customers, a Major Incident Response Process is invoked ensuring rapid issue identification, Diagnosis, Containment, Resolution and Recovery. In addition to automated processes that respond directly to disaster recovery scenarios, Heartland has the people and processes in place to ensure maximum system availability 24 X 7.

Heartland School Solutions
Major Incident Response Process (MIRP)



Heartland MySchoolApps Data Security and Privacy Plan

Purpose
The purpose of this document is to describe the plan for ensuring that protected data entrusted to Heartland remains secure.

Scope
Heartland is responsible for protecting data for our hosted service offerings, including MySchoolApps. Hosted services are those that process data off customer premise in Heartland managed data centers.

Executive Summary
Heartland seeks to provide a secure computing environment for its hosted service offerings. Heartland maintains reasonable administrative, technical and physical safeguards to protect the confidentiality of all information transmitted online, including but not limited to encryption, firewalls, password protection, and Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Heartland has implemented policies and practices pursuant to various security rules and regulations relating to the security and safeguarding of protected data.

Definitions
"Personally Identifiable Information" or "PII" refers to data that is classified as confidential by State and federal law and is therefore considered "Protected Data". PII utilized by MySchoolApps is limited and includes the student's name; the name of a student's parent; guardian or other family member; the address of a student or a student's family; various meal program eligibility conditions and income. Heartland meets or exceeds requirements for protecting personally identifiable information as defined by the Family Educational Rights and Privacy Act , 20 U.S.C. 1232g, and the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103. Heartland will use data collected for the purpose of fulfilling its duties under the Heartland solution license agreement, and will not share such data with or disclose it to any third party except as provided for in the agreement, as required by law, or if authorized in writing by the District.

Data Security
Heartland will store and process MySchoolApps data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in FIPS PUB 200, to secure such data from unauthorized access, disclosure, alteration, and use. Heartland ensures that all such safeguards, including the manner in which parent and student data is collected, accessed, used, stored, processed, disposed of and disclosed, will comply with all applicable federal and state data protection and privacy laws, regulations and directives, as well as the terms outlined in the MySchoolApps privacy policy.

In the event of a security breach, if permitted by law and law enforcement, that resulted in unauthorized access to or disclosure or use of system data, Heartland will notify the appropriate districts in writing, fully investigate the incident, cooperate fully with the district's investigation of and response to the incident, and use best efforts to prevent any further Security Breach at Heartlands expense in accordance with applicable privacy laws. Except as otherwise required by law, Heartland will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the District.

MySchoolBucks Privacy Policy

MySchoolBucks Privacy Policy https://www.myschoolbucks.com/ver2/etc/getprivacy ("Site")

Last Updated: March 6, 2017

Heartland Payment Systems, Inc. ("Heartland," "we," "us," "our") recognizes the importance of maintaining effective privacy practices. Among other topics, this Privacy Policy together with the Site's Terms of Use explains:

1. What type of Personal Information we collect about visitors or users of our websites, mobile applications, and online services linked to this Privacy Policy(collectively referred to herein as the "Services");
2. How we collect Personal Information;
3. How we use Personal Information;
4. Who we share Personal Information with; and
5. How we store and protect Personal Information.

By using the Services, you accept and agree to the terms and conditions of this Privacy Policy. If you do not wish to agree to this Privacy Policy, please do not use the Services and do not provide any information about you to us.

We will routinely update this Privacy Policy to clarify our practices and to reflect new or different privacy practices, such as when we add new services, functionality or features to the Services. Updates may be with or without notice, and we recommend you visit this page frequently to review changes. You can determine when this Privacy Policy was last revised by referring to "Last Updated" above. Any changes to this Privacy Policy will be effective upon posting on this Site.

GLOSSARY OF TERMS USED

"**Affiliate**" means a company owned and/or controlled by Heartland.

"**Business Partners**" means, collectively, third parties with whom we conduct business.

"**Cookie**" means a small amount of information that a web server sends to your browser that stores information about your account, your preferences, and your use of the Services. Some cookies are temporary, whereas others may be configured to last longer. Session Cookies are temporary cookies used for various reasons, such as to manage page views. Your browser usually erases session cookies once you exit your browser. Persistent Cookies are more permanent cookies that are stored on your computers or mobile devices even beyond when you exit your browser.

"**Device Data**" means information concerning a device you use to access, use, or interact with the Services, such as operating system type or mobile device model, browser type, domain, and other system settings, the language your system uses and the country and time zone of your device, geo-location, unique device identifier or other device identifier, mobile phone carrier identification, and device software platform and firmware information.

"Non-Identifying Information" means information that alone cannot identify you, including data from Cookies, Pixel Tags and Web Beacons, and Device Data. Non-Identifying Information may be derived from Personal Information.

"Other Sources" means sources of information that legally provide Heartland with your information, and which are outside the scope of this Privacy Policy at the time of collection.

"Partner or School" means a school, school district, or organization of schools or school districts for which Heartland provides the Services.

"Personal Information" means information about you that specifically identifies you or, when combined with other information we have, can be used to identify you. This includes the following types of information: (1) contact information, including your name, postal addresses, email addresses, telephone numbers, or other addresses at which you are able to receive communications; (2) financial information, including information collected from you as needed to process payments and to administer your participation in the Services. We collect such information as your payment card number, expiration date, and card verification number; and (3) demographic information related to billing. For certain school districts, you as the parent of a student may also provide the student's (1) first and last names, (2) student identification number and (3) school attending.

"Pixel Tags and Web Beacons" means tiny graphic images placed on website pages or in our emails that allow us to determine whether you have performed specific actions.

"Services" means the payment terminals, websites, mobile applications, or online services owned or operated by Heartland and its Affiliates linked to this Privacy Policy.

"Vendors" means, collectively, third parties that perform business operations on behalf of Heartland, such as transaction processing, billing, mailing, communications services (e-mail, direct mail, etc.), data processing and analytics.

INDEX OF TOPICS ADDRESSED IN THIS PRIVACY POLICY

1. HOW HEARTLAND COLLECTS INFORMATION

We will collect information, including Personal Information and Non-Identifying Information, when you interact with us and the Services, such as when you:

- access or use the Services;
- register, subscribe, or create an account with us;
- open or respond to our e-mails or communicate with us;
- provide information to enroll or participate in programs provided on behalf of, or together with, Schools or Business Partners; and
- visit any page online that displays our ads or content.

We also may collect Personal Information when you contact us via email or our online customer service options.

We may receive information from Other Sources. Heartland will use such information in accordance with applicable laws. Such information, when combined with Personal Information collected as provided in this Privacy Policy, will also be handled in accordance with this Privacy Policy. We also use Cookies, Pixel Tags and Web Beacons, local shared objects, files, tools and programs to keep records, store your preferences, and collect Non-Identifying Information, including Device Data and your interaction with the Services and our Business Partners' web sites.

We use Cookies that contain serial numbers that allow us to connect your use of the Services with other information we store about you in your profile or as related to your interactions with the Services. We use Session Cookies on a temporary basis, such as to manage your view of pages on the Services. We use Persistent Cookies for a number of purposes, such as retrieving certain information you have previously provided (for example, your user id if you asked to be remembered). Information from Cookies also tells us about the website you were visiting before you came to the Services and the website you visit after you leave the Services.

When you access these pages or open email messages, we use Pixel Tags and Web Beacons to generate a notice of that action to us, or our Vendors. These tools allow us to measure response to our communications and improve the Services.

Device Data may be collected when your device interacts with the Services and Heartland, even if you are not logged into the Services using your device. If you have questions about the security and privacy settings of your mobile device, please refer to instructions from your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

Because we do not track our Site's users over time and across third-party sites, we do not respond to browser do not track signals at this time.

2. HOW HEARTLAND USES INFORMATION

We (or our Vendors on our behalf), use information collected as described in this Privacy Policy to:

- Operate, maintain and improve the Services;
- Facilitate transactions you initiate or request through the Services;
- Answer your questions and respond to your requests;

- Communicate and provide additional information that may be of interest to you concerning your chosen Services. Send you reminders, technical notices, updates, security alerts, support and administrative messages, service bulletins, and requested information.
- If you elect to participate, administer rewards, surveys, contests, or other promotional activities or events sponsored by us or our Business Partners;
- Manage our everyday business needs, such as administration of our Services, analytics, fraud prevention, and enforcement of our corporate reporting obligations and Terms of Use, or to comply with applicable state and/or federal law;
- Enhance other information we have about you directly or from Other Sources to help us better provide your chosen Services to you.

We also may use information collected as described in this Privacy Policy with your consent or as otherwise required by state and/or federal law.

3. WHEN AND WHY HEARTLAND DISCLOSES INFORMATION

We (or our Vendors on our behalf) may share your Personal Information as required or permitted by the School to provide the Services in compliance with the federal Family Educational Rights and Privacy Act and/or other applicable state and/or federal law. We may share your Personal Information:

- With Schools in which the student is or has been affiliated.
- with any Heartland Affiliate which may only use the Personal Information for the purposes described in this Privacy Policy;
- with our Vendors to provide services for us and who are required to protect the Personal Information as provided in this Privacy Policy;
- with a purchaser of Heartland or any of Heartland Affiliates (or their assets);
- to comply with legal orders and government requests, or as needed to support auditing, compliance, and corporate governance functions;
- to combat fraud or criminal activity, and to protect our rights or those of our Affiliates, users, and Business Partners, or as part of legal proceedings affecting Heartland;
- in response to a subpoena, or similar legal process, including to law enforcement agencies, regulators, and courts in the United States and other countries where we operate;
- Upon your consent or election to participate, with any third party for any reason.

4. SECURITY OF PERSONAL INFORMATION

Heartland maintains reasonable administrative, technical and physical safeguards to protect the confidentiality of information transmitted online, including but not limited to encryption, firewalls and SSL (Secure Sockets Layer). Heartland has implemented policies and practices pursuant to various security rules and regulations relating to the security and safeguarding of payment cardholder data, including the Payment Card Industry Data Security Standards (PCI-DSS).

To ensure that the only individuals and entities who can access Personal Information are those that have been specifically authorized by Heartland to access Personal Information, Heartland has implemented various forms of authentication to identify the specific individual who is accessing the information. Heartland individually determines the appropriate level of security that will provide the necessary level of protection for the Personal Information it maintains. Heartland does not allow any individual or entity unauthenticated access to Personal Information at any time.

Heartland is not liable for loss resulting from the loss of passwords due to user negligence. If you believe your password has been lost or compromised, we recommend that you immediately change your password.

5. DATA ANONYMIZATION AND AGGREGATION.

Subject to your consent if required by law, we may anonymize or aggregate your personal information in such a way as to ensure that you are not identified or identifiable from it, in order to use the anonymized or aggregated data, for example, for statistical analysis and administration including analysis of trends, to carry out actuarial work, to tailor products and services and to conduct risk assessment and analysis of costs and charges in relation to our products and services. We may share anonymized or aggregated data with our affiliates and with other third parties. This policy does not restrict our use or sharing of any non-personal, summarized, derived, anonymized or aggregated information (i.e., volumes, totals, averages, etc.).

6. THIRD-PARTY WEBSITES AND SERVICES

This Privacy Policy only addresses the use and disclosure of information by Heartland through your interaction with the Services. Other websites that may be accessible through links from the Services may have their own privacy statements and personal information collection, use, and disclosure practices. Our Business Partners may also have their own privacy statements. We encourage you to familiarize yourself with the privacy statements provided by these other parties prior to providing them with information.

7. YOUR CHOICES

In addition, you may choose to unsubscribe from promotional email messages by using the unsubscribe instructions at the bottom of promotional emails. Please note that even if you unsubscribe from promotional email messages, we may still need to contact you with important transactional information related to your account. For example, even if you have unsubscribed from our promotional email messages, we will still send you confirmations when you utilize the Services.

You may manage how your browser handles Cookies by adjusting its privacy and security settings. Browsers are different, so refer to instructions related to your browser to learn about cookie-related and other privacy and security settings that may be available.

You may manage how your mobile device and mobile browser share certain Device Data with Heartland, as well as how your mobile browser handles Cookies by adjusting the privacy and security settings on your mobile device. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

If you wish to stop receiving offers directly from our Business Partners, with whom you have elected to participate, you can follow the unsubscribe instructions in the emails that they send you.

8. ACCESSING PERSONAL INFORMATION; RETENTION OF DATA

For some of our Services, you may access, update and delete information in your profile by logging into your account and accessing your account profile.

If you have questions or requests related to your information, please contact us as set forth in Section 13 below. While we are ready to assist you, please note that we cannot always delete records. For example, we are required to retain records relating to certain transactions involving the Services for financial reporting and compliance reasons. We will retain your Personal Information for as long as your account is active or as needed to provide you with the Services and to maintain a record of your transactions for financial reporting purposes. We will retain and use your Personal Information only as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

9. SOCIAL NETWORKS

The Services may be accessible through or contain connections to areas where you may be able to publicly post information, communicate with others such as discussion boards or blogs, review products and merchants, and submit media content. Prior to posting in these areas, please read our Terms of Use carefully. All the information you post may be accessible to anyone with Internet access, and any Personal Information you include in your posting may be read, collected, and used by others. For example, if you post your email address along with a public restaurant review, you may receive unsolicited messages from other parties. You should avoid publicly posting Personal Information or identifying information about third parties.

10. NOTICE TO RESIDENTS OF COUNTRIES OUTSIDE THE UNITED STATES OF AMERICA

If you live outside the United States (including in the EEA/CH), and you use the Services or provide us with Personal Information directly via the Services, your information will be handled in accordance with this Privacy Policy. By using the Services or giving us your Personal Information, you are directly transferring your Personal Information and Non-Identifiable Information to us in the United States. The United States may not have the same level of data protection as your jurisdiction. However, you agree and consent to our collection, transfer, and processing of your Personal Information and Non-Identifiable Information in accordance with this Privacy Policy. You are solely responsible for compliance with any data protection or privacy obligations in your jurisdiction when you use the Services or provide us with Personal Information. Regardless of where we transfer your information, we still protect your information in the manner described in this Privacy Policy.

11. CALIFORNIA PRIVACY RIGHTS

Pursuant to Section 1798.83 of the California Civil Code, residents of California can obtain certain information about the types of personal information that companies with whom they have an established business relationship have shared with third parties for direct marketing purposes during the preceding calendar year. In particular, the law provides that companies must inform consumers about the categories of personal information that have been shared with third parties, the names and addresses of those third parties, and examples of the types of services or products marketed by those third parties. To request a copy of the information disclosure provided by Heartland pursuant to Section 1798.83 of the California Civil Code, please contact us via the email or address stated above. Please allow 30 days for a response.

Heartland complies with California Assembly Bill No. 1584 and California Senate Bill No. 1177.

12. CHILDREN'S PRIVACY

Heartland does not intend that any portion of the Services will be accessed or used by children under the age of thirteen, and such use is prohibited. The Services is designed and intended for adults. By using Heartland's Services, you represent that you are at least eighteen years old and understand that you must be at least eighteen years old in order to create an account and utilize the Services. We will promptly delete information associated with any account if we obtain actual knowledge that it is associated with a registered user who is not at least eighteen years old.

13. CONTACT US

The Site is operated by Heartland Payment Systems, Inc.
Our postal address is
570 Devall St., Suite 202
Auburn, Alabama 36830

We can be reached via email at support@myschoolbucks.com or you can reach us by telephone at 1-855-832-5226.

If you feel that this site is not following its stated information policy, you may contact us at the above addresses or phone number.