CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Newport-Mesa Unified School District

and

Heartland School Solutions

09/06/2017

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Newport-Mesa USD (hereinafter referred to as "LEA") and Heartland School Solutions (hereinafter referred to as "Provider") on September 6, 2017. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated September 6, 2017 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; 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", agrees 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 privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. 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. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

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

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated 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 or any other Pupil Records 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 Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or any other Pupil Records 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 personally identifiable information on 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 reasonably timely manner to the LEA's request for personally identifiable information 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 Pupil Records of 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.** Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.

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 redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA.** LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.

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

3. **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.

4. **District Representative.** At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

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

2. **Authorized Use.** The data shared 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.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the 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. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures 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 in Exhibit "D" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by 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. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

    b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was

obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices 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 computer 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.

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, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement

g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors 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 assessments of Subprocessors to determine their compliance with this Article.

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

      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 the agency 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. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.

e. At the request and with the assistance of the District, 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.

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 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.

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).

4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this 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, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

6. **Application of Agreement to Other Agencies.** Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.

7. **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.

8. **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.

9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF 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 LOCATED IN Orange COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[*Signature Page Follows*]

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

Newport-Mesa Unified School District

Date: ~~09/06/2017~~ 9/13/2017

Printed Name: Russell Lee-Sung

Title/Position: Deputy Superintendent, CAO

Heartland School Solutions

Date: 09/06/2017

Printed Name: Terry Roberts

Title/Position: President School Solutions

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

MySchoolBucks is an online e-payment system designed specifically for use in the K-12 market and provides schools, both public and private, with a solution that is easy to use, powerful and secure. MySchoolBucks is designed to be a single solution for all school-related payments, including transportation. With the ability to designate a separate bank account for each item, reporting and reconciliation are simple and straightforward.

In addition to online payments, MySchoolBucks can also facilitate the collection of in-person credit card payments with MySchoolBucks Anywhere. MySchoolBucks Anywhere transforms any Apple iPad into a mobile point-of-sale with our app and proprietary card reader. MySchoolBucks Anywhere is completely integrated with MySchoolBucks, allowing schools to manage all in-person payments and online sales from a single, full-feature management portal designed to facilitate electronic payment for any school-related fee(s).

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)	✓
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	✓
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	✓
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	✓
	Email	✓
	Phone	✓
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓

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	✓
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	✓
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.	

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/performance scores	☐
	Other transcript data -Please specify:	☐

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data - Please specify:	☐
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.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 1177, SOPIPA, 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 AB 1584.

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, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

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 Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

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 local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 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 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or 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.

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "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. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

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" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) 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"

DATA SECURITY REQUIREMENTS

Please reference the "MySchoolBucks Agreement" document immediately following Page 22 for additional information.

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Newport-Mesa USD and which is dated September 6, 2017 to any other LEA ("Subscribing LEA") to anywho accepts this General Offer though 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 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 statutes; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Heartland School Solutions

Date: September 6, 2017

Printed Name: Terry Roberts

Title/Position: President 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 Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Date:

Printed Name:

Title/Position

EXHIBIT D

MySchoolBucks Agreement:

6. SECURITY OF PERSONAL IDENTIFIABLE INFORMATION

6.1 HPS agrees that any and all Personal Identifiable Information will be stored and maintained in a secure location and solely on designated servers. No Personal Identifiable Information, at any time, will be processed on or transferred to any portable computing device or any portable storage medium, unless the data is encrypted at rest or that storage medium is in use as part of the HPS' designated support, backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the Service shall be contained within the United States unless an alternate location is specifically agreed to, in writing, by the School. Notwithstanding the foregoing, a User of the application, may retrieve Personal Identifiable Information associated with the account, from portable and non-portable devices alike. Personal Identifiable Information, collected from the Services' Users, whether via letter, voice, fax, email, chat, SMS, social media, mobile application, or browser, will be handled in accordance with MySchoolBucks Terms of Use and Privacy Policy.

6.2 HPS maintains reasonable administrative, technical and physical safeguards to protect the confidentiality of information transmitted online, including but not limited to encryption, firewalls, Secure Sockets Layer (SSL). HPS has implemented policies and practices pursuant to various security rules and regulations relating to the security and safeguarding of payment data, including the Payment Card Industry Data Security Standards (PCI-DSS). However, no precautions, means, or method of transmission which uses the internet or method of storage is absolutely 100% secure.

6.3 When sharing Personal Identifiable Information with its Affiliates, HPS will require those Affiliates to comply with this Agreement.

6.4 All of HPS' personnel are trained on information security. HPS' information security policy requires that all personnel who come into contact with School Data receive training on the proper techniques for handling such data. Such training is required on at least an annual basis.

6.5 Users may supply data, including confidential data, to utilize the Services. The MySchoolBucks Terms of Use and Privacy Policy govern the sharing of data supplied by MySchoolBucks Users.

7.5 HPS agrees that, upon the School's request, if this Agreement is terminated or upon expiration, HPS shall erase, destroy, and render unreadable, all School Data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities. HPS shall certify in writing that these actions have been completed within thirty (30) days from receipt of the request by the School. Notwithstanding the foregoing, School Data may be retained or available to HPS upon termination of the Agreement if a student, parent or legal guardian of a student chooses to maintain an electronic account with HPS which requires the storing of School Data.

MySchoolBucks Privacy Policy:

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 emails 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 Heartlands 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