

# Standard Student Data Privacy Agreement for Heartland School Solutions

## Vendor-specific DPA

Park Ridge-Niles Community Consolidated School District 64 or LEA

and

Heartland Payment Systems, LLC

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Park Ridge-Niles Community Consolidated School District 64, located at 164 S. Prospect Ave, Park Ridge, IL 60068 (the “**Local Education Agency**” or “**LEA**”) and Heartland Payment Systems, LLC, located at 765 Jefferson Rd #400, Rochester, NY 14623 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), including but not limited to the Illinois School Student Records Act (“**ISSRA**”), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act (“**MHDDCA**”), 740 ILCS 110/, Student Online Personal Protection Act (“**SOPPA**”), 105 ILCS 85/, Identity Protection Act (“**IPA**”), 5 ILCS 179/, and Personal Information Protection Act (“**PIPA**”), 815 ILCS 530/, and Local Records Act (“**LRA**”), 50 ILCS 205/, and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in this Agreement.

**2. Special Provisions. Check if Required**

If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA for so long as the Services are being provided to the LEA or as long as Provider has any Student Data, whichever is longer. An agreement formed by a Subscribing LEA's acceptance of Exhibit E shall remain in effect as between Provider and Subscribing LEA for so long as the Services are being provided to the Subscribing LEA or as long as Provider has any Student Data, whichever is longer.

4. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "Services").

5. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Mary Jane Warden

Title: Privacy Officer

Address: 164 S. Prospect Ave, Park Ridge, IL 60068

Phone: 847-318-4300

Email: privacy@d64.org

The designated representative for the Provider for this DPA is:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

Email: \_\_\_\_\_

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**LEA:**

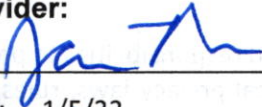
By: 

Date: 1/5/2022

Printed Name: Mary Jane Warden

Title/Position: Privacy Officer

**Provider:**

By: 

Date: 1/5/22

Printed Name: Jeremy Loch

Title/Position: SVP & General Manager, School Solutions

## 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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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, as described in FERPA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

**2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.

**3. 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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

**1. Student Data Property of LEA.** All Student Data transmitted to the Provider by LEA pursuant to the Services 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 by the LEA, including any modifications or additions or any portion thereof from the LEA, are subject to the provisions of this DPA 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 provided by LEA under 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 LEA as it pertains to the use of Student Data, notwithstanding the above. To the extent that Provider receives Student Data from a Parent or other End User directly (as opposed to through the LEA), the Parties agree and understand that a separate agreement between Provider and the Parent or other End User will govern the obligations of the Provider to those third parties with respect to that specific information.

**2. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student 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 Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student Generated Content to a separate account created by the student.

**4. Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant

to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

**5. Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

**1. Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

**2. Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 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 Student Data.

**4. Unauthorized Access Notification.** LEA shall notify Provider promptly (within 72 hours of confirmation of the incident) of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

**2. Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

**3. Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student 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 acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA, this DPA, or applicable law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully

issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

**5. De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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 the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

**6. Disposition of Data.** Following expiration or termination of the Service Agreement, including the DPA, and upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. If LEA does not request Provider to return or destroy the Student Data, then Provider will dispose of the Student Data in accordance with applicable privacy laws, and in the normal course of business. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The Parties may mutually agree to employ and execute a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."

**7. Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

**8. Subcontractors.** By no later than 5 business days after the date of execution of this DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA following its written request, by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

## ARTICLE V: DATA PROVISIONS

**1. Data Storage.** Where required by applicable law, Student Data shall be stored within the United States.

**2. Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA and subject to a separate nondisclosure agreement, the Provider will provide the LEA with a copy of its most current SSAE 16/18 report regarding the third party audit of security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA where and to the extent required by applicable law.

**3. Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement and maintain reasonable security practices and procedures that otherwise meet or exceed industry standard designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure. Provider has implemented NIST Cybersecurity Framework Version 1.1. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

**4. Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider and requiring notification of the data subject under applicable law the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation that the notification is required to be made, or sooner if required by applicable law. Incidents not resulting in the legally required notification of data subjects will be made as expeditiously as possible and without unreasonable delay unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

- i. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- ii. 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.
- iii. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- iv. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
- v. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

- (2) Provider agrees to adhere to all federal and state requirements 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.
- (3) Provider further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and 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 and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians, unless Provider is legally required to do so by applicable law.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

**5. Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach occurring through Provider or any of its products, the Provider agrees to notify LEA promptly and in accordance with applicable law, if legally permitted to do so. In the event of a Security Breach that is solely attributable to the Provider or its SubProcessors, the Provider agrees to and assume responsibility for informing all affected individuals in accordance with applicable law, and to indemnify, hold harmless and defend the LEA's Board of Education and each of its individual Board members, Board officers, employees, agents, representatives, insurers, successors, and assigns from and against any and all claims, damages, or causes of action directly related to the unauthorized release, including but not limited to costs and expenses associated with:

- a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
- b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
- d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

**6. Indemnification for Breach of Data Provided to Provider by Parent.** Provider agrees to indemnify, defend, and hold harmless the Board of Education and each of its individual Board members, Board officers, employees, agents, representatives, insurers, successors, and assigns from and against any and all claims, demands, charges, complaints, causes of action, fines and penalties (including, but not limited to, attorney's fees), and other liability arising from, related to, or connected in any way with a security breach related to any data Provider receives directly from a Parent or other End User via Provider's website or application.

## **ARTICLE VI: ILLINOIS PROVISIONS**

**1. Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act



("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

**2. School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest. The authorized purpose under this DPA shall be the Services outlined in the Contract. However, with respect to low income and free and reduced price eligibility information of students, Provider is expressly limited to use of such information with respect to administration of the LEA food service program as required by 42 USC 1758 and implementing regulations.

**3. Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA, the data holder, or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall, unless prohibited by law, redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall, unless prohibited by law, notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

**4. Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

**5. Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

**6. Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

**7. Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including

but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of this DPA, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

**8. Transfer or Deletion of Student Data.** The Provider shall review, in accordance with applicable law and operational policy, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. Transfer or deletion of Student Data shall occur in accordance with Article IV Section 6 above. If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request. Any provision of Student Data to the LEA from the Provider shall be transmitted in a mutually agreeable format readable by the LEA.

**9. Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including all Exhibits.

**10. Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document. Provider's terms of user and privacy policy can be found at [myschoolbucks.com](http://myschoolbucks.com)

**11. Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

**12. Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

## **ARTICLE VII: GENERAL OFFER OF 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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## **ARTICLE VIII: MISCELLANEOUS**

**1. Termination.** In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.

**2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

**3. Priority of Agreements.** This DPA shall govern the treatment of Student Data Provider receives from LEA in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service 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.

**4. Entire Agreement.** This DPA and the Service Agreement constitute 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.

**5. 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.

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

**7. 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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

**8. Authority.** Each party represents that it is authorized to bind to the terms of this DPA, 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.

**9. Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

Heartland provides software solutions that support school functions such as meal ordering, online payment and ordering, point of sale transactions, transportation, activities, spirit wear, and other items as configured by LEA. Heartland also provides nutrition services operations and accountability software solutions, including applying for subsidized meals. This DPA applies to all software solutions provided by Heartland, including Mosaic.

**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 Assessment	Meta data on user interaction with application	√
	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data – attendance at a meal is captured	√
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	√
Conduct	Conduct or behavioral data	
Demographics (School can configure which data points to use)	Date of Birth	√
	Place of Birth	
	Gender	√
	Ethnicity or race (for nutritional services)	√
	Language information (native, or primary language spoken by student)	√

	Other demographic information-Please specify: School can configure registration or forms and collect additional demographic info, but the services do not automatically collect this information	
Enrollment	Student school enrollment	√
	Student grade level	√
	Homeroom	√
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	√
	Other enrollment information-Please specify: class schedule	√
Parent/Guardian Contact Information (for MSB, parent provides directly via separate terms of service)	Address	√
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last – for nutrition services	√
Schedule	Student scheduled courses	
Schedule Special Indicator	Teacher names	
	English language learner information	
Special Indicator Student Contact Information	Low income status	√
	Medical alerts/ health data	√

	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care) (to the extent included in the nutritional services application)	√
	Other indicator information-Please specify:	
	Address – collected for nutrition services	√
Student Contact Information Student Identifiers (School can configure which data points to use)	Email	√
	Phone	√
	Local (School district) ID number	√
Student Identifiers Student Name (MSB allows a parent to establish a student account after consent to terms and conditions)	State ID number	
	Provider/App assigned student ID number	√
	Student app username	
	Student app passwords	
	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.	



Student work	Other student work data -Please specify: District can configure forms to collect additional information	√
Transcript	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: District can choose to create a form to collect this information	√
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

## **EXHIBIT “C”** **DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, enabling parents to make school-related payments, place lunch orders, and that also provides nutritional information. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Student Generated Content:** The term “Student-Generated Content” means materials or content created by a student in the services 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 student content.

**School Official:** For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re disclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract.

**Student Data:** Student Data includes any data provided by LEA that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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,

individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data also includes, where applicable, any information so defined under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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. Student Data does not include data that Provider receives directly from a parent, or guardian related to parent or guardian or billing information, through the MSB website or application.

**Subprocessor:** For the purposes of this DPA, 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 service, and who has access to Student Data.

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

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**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 Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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**

Provider 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:

**1. Extent of Disposition**

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Disposition is Complete. Disposition extends to all categories of data.

**2. Nature of Disposition**

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**3. Schedule of Disposition**

Data shall be disposed of by the following date:


As soon as commercially practicable.

By

**4. Signature**

\_\_\_\_\_ Authorized Representative of LEA

**5. Verification of Disposition of Data**

 \_\_\_\_\_ Authorized Representative of Company

1/5/22 Date

\_\_\_\_\_ 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 ("Originating LEA") which is dated January 5, 2022, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("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 Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing 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. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: \_shelley.lorren@e-hps.com and support@myschoolbucks.com.

**PROVIDER:**

BY: Jeremy Loch- 

Date: 1/5/22

Printed Name: Jeremy Loch

Title/Position: SVP & General Manager

**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 for a term of \_\_\_\_\_.

**\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA:**

BY: \_\_\_\_\_

Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

**DESIGNATED REPRESENTATIVE OF LEA:**

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_

Email: \_\_\_\_\_