OK AS TO FORM
MM @ WC 2.24.2021

Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

Heartland Payment Systems, LLC dba Heartland School Solutions

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and ***Heartland Payment Systems, LLC dba Heartland School Solutions***, a limited liability company organized under the laws of Delaware. ("Services Provider") describes the services to be provided to JCPS by Services Provider, and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of March 10, 2021 and will terminate when the services contract referenced in Paragraph B.1. below terminates, unless terminated earlier by either party pursuant to Section H.

B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following services to JCPS under the terms of a services contract between JCPS and Services Provider effective March 10, 2021: MCS software conversion from district on premises to the Heartland School Solutions cloud offering for the applications Newton, Franklin, Edison and DataCenter.

2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

3. JCPS shall disclose to Services Provider, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3,

under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The confidential data, including student and non-student information to be disclosed, is described in a document attached to this agreement as **Attachment A.** Services Provider shall use personally identifiable information from education records and other records in order to perform the services described in Paragraph B.1 above. Services Provider shall notify JCPS and JCPS shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the services or any changes to the scope, purpose or duration of the services themselves. Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the services contract described in Paragraph B.1 above.

4. Services Provider and JCPS shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. Services Provider shall confirm the transfer of confidential data and notify JCPS as soon as practicable of any discrepancies between the actual data transferred and the data described in this Agreement. The same protocol shall apply to any transfer of confidential data from Services Provider to JCPS.

C. CONSTRAINTS ON USE OF DATA

1. Services Provider agrees that the services shall be provided in a manner that does not permit personal identification of parents and students by individuals other than representatives of Services Provider that have legitimate interests in the information.

2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS.

3. Services Provider shall not re-disclose any individual–level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS, unless legally prohibited from doing so.

4. Services Provider shall use the data only for the purpose described in Paragraph B.1 above, including to improve the services. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to

comply with all applicable Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any data regarding any JCPS student that is subject to FERPA, Services Provider agrees to:

    a. In all respects comply with the provisions of FERPA.

    b. Use any such data for no purpose other than to fulfill the purposes of the services contract described in Paragraph B.1 above, and not share any such data with any person or entity other than Services Provider and its employees, contractors and agents, without the prior written approval of JCPS.

    c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.

    d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data expect as necessary to fulfill the purposes of the services contract described in Paragraph B.1 above.

    e. Provide the services under the services contract described in Paragraph B.1 above in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agents of Services Provider having a legitimate interest in knowing such personal identification.

    f. Upon request from JCPS, Services Provider will destroy or return to JCPS any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Services Provider for the purposes of the services contract described in Paragraph B.1 above. JCPS acknowledges that Services Provider may be required to retain certain information for legal, regulatory, or audit purposes, in which case the information will be retained subject to the protections herein.

3. Services Provider shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Services Provider becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall, subject to any

applicable legal prohibition, use all reasonable efforts to provide JCPS with prior notice before disclosure so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of confidential and otherwise personally identifiable data that Services Provider is legally required to disclose.

4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data.

5. Services Provider shall not use data shared under this Agreement for any purpose other than the services contract described in Paragraph B.1 above. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the data to Services Provider.

6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include, but are not limited to:

    a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;

    b. Encrypting all data carried on mobile computers/devices;

    c. Encrypting data before it is transmitted electronically;

    d. Requiring that users be uniquely identified and authenticated before accessing data;

    e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the data necessary for this to perform their job functions;

    f. Ensuring that all staff accessing data sign a nondisclosure statement, attached as **Attachment B**, and maintain copies of signed statements;

    g. Securing access to any physical areas/electronic devices where sensitive data are stored;

h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and

i. Installing anti-virus software to protect the network.

7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

   a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

      i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

      ii. A Social Security number;

      iii. A taxpayer identification number that incorporates a Social Security number;

      iv. A driver's license number, state identification card number or other individual identification number issued by an agency;

      v. A passport number or other identification number issued by the United States government; or

      vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

   b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.

   c. Other than as necessary to provide the Services, Services Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.

d. Services Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Services Provider agrees that:

   a. Services Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Services Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

   b. Pursuant to KRS 365.734(2), Services Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

   c. Pursuant to KRS 365.734(2), Services Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

   d. Pursuant to KRS 365.734(3), Services Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

9. Services Provider shall report all known or suspected breaches of the data, in any format, to Dr. Kermit Belcher, Chief Information Officer. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, a breach of hard copies of records, etc.); (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.

10. Services Provider shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement. Services Provider agrees to require all employees, contactors, or agents of any kind using JCPS data to comply with this provision. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the data has been destroyed.

11. For purposes of this agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates Tyson Prescott, Senior Director, Research & Development (or an alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. JCPS or its agents may, upon request, review the records Services Provider is required to keep under this Agreement.

12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of protected student information constitutes just cause for JCPS to immediately terminate this Agreement.

13. Services Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of $5M. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, Kentucky 40218

14. Services provider shall maintain, during the term of this Agreement, ISO27001 or SOC2 certification. If Services Provider is unable to provide ISO27001 or SOC2 certification, minimum requirements on a JCPS-provided standardized questionnaire must be met. Upon request, Services Provider shall furnish a current ISO27001, SOC2 certification, or updated questionnaire.

E. FINANCIAL COSTS OF DATA-SHARING

Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student data requested under this agreement and costs associated with the electronic delivery of the student data to Services Provider.

No payments will be made under this Agreement by either party. Any payments to Services Provider will be made under the services contract described in Paragraph B.1 above.

F. OBLIGATIONS OF JCPS

During the term of this Agreement, JCPS shall:

1. Prepare and deliver the data described in **Attachment A**.

G. LIABILITY

Services Provider agrees to be responsible for and assumes all liability for any third party claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Services Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims"). Services Provider agrees to hold harmless JCPS and pay any reasonable third party costs incurred by JCPS in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this Agreement.

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):

    a. By either party in the event of a material breach of this Agreement by another party provided however, the breaching party shall have thirty (30) days to cure such breach and this Agreement shall remain in force.

    b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.

2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, within seven (7) days of the termination the confidential information shall be returned or destroyed within seven (7) days of the termination and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after the end of the term, Services Provider shall return or destroy all confidential information and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11.

3. Destruction of the confidential information shall be accomplished by utilizing an approved method of confidential destruction, including but not limited to shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer. If new materials are developed during the term of the services contract described in Paragraph B.1 above, ownership and copyright of such will be governed by the terms of the services contract.

J. MODIFICATION

No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

K. BREACH OF DATA CONFIDENTIALITY

Services Provider acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to JCPS for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by Services Provider, JCPS, in addition to any other rights and remedies available to JCPS at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that Services Provider has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), JCPS may not allow Services Provider access to personally identifiable information from its education records for at least five (5) years.

L. CHOICE OF LAW AND FORUM

This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky. Any action or Claim arising from, under or pursuant to this Agreement shall be brought in the Jefferson County, Kentucky, Circuit Court, and the parties expressly waive the right to bring any legal action or Claims in any other courts.

M. WAIVER

No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right or prevent a similar subsequent act from constituting a violation of this Agreement.

N. SEVERABILITY

If any part of this Agreement is held to be void, against public policy or illegal, the balance remaining provisions of this Agreement shall continue to be valid and binding.

O. NOTICES

Any notices or reports by one party to the other party under this Agreement shall be made in writing, to the address shown in the signature portions of this Agreement, or to such other address as may be designated in writing by one party to the other. Notices

shall be effective when received if personally delivered, or three days after mailing if mailed.

P. RELATIONSHIP OF PARTIES

JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

Q. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Services Provider shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of JCPS, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

Heartland Payment Systems, LLC dba Heartland School Solutions ATTN: Shelley R. Lorren
113 Heritage Blvd
Covington, LA 70433

BY: 

Name: Jeremy Loch

Title: Senior VP/General Manager, School Solutions

Date: 1/25/21

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: _____

Name: Martin A. Pollio, Ed. D.,

Title: Superintendent

Date: _____

Attachment A

CONFIDENTIAL INFORMATION TO BE DISCLOSED

- Employee First Name
- Employee Middle Initial
- Employee Last Name
- Employee Suffix
- Guardian First Name
- Guardian Middle Initial
- Guardian Last Name
- Guardian Suffix
- Guardian Income
- Guardian Date of Birth
- Guardian Email Address
- Guardian Physical Address
- Guardian Phone #'s
- Guardian Truncated SSN (4 digits)
- Student Nickname
- Student First Name
- Student Middle Initial
- Student Last Name
- Student Suffix
- Student Nickname
- Student Number
- Student School
- Student Physical Address
- Student Phone #'s,
- Student Data of Birth
- Student Truncated SSN (4 digits)
- Student Ethnicity,
- Student Application Meal Status
- Student Allergens
- Student Grade
- Student Gender
- SNAPTTANF/Medicaid,
- Guardian/Student Email Address
- Guardian/Student Physical Address
- Guardian/Student Phone ifs
- Guardian Truncated SSN (4 digits)