OK AS TO FORM
AMH 7-25-2024

AMENDMENT TO DATA PRIVACY AGREEMENT

THIS AMENDMENT TO DATA PRIVACY AGREEMENT (hereinafter "Amendment") is entered by and between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools (hereinafter "JCPS") with its principal place of business located at 3332 Newburg Road, Louisville, Kentucky 40218, and National Student Clearinghouse, with its principal place of business located at 2300 Dulles Station Blvd, Suite 220, Herndon, VA 20171 (hereinafter "Provider").

WHEREAS, The Parties have entered into a Data Privacy Agreement between JCPS and Provider dated June 28, 2023, which provided for the sharing of data between JCPS and Provider (the "Agreement"); and

WHEREAS, the Parties wish to amend the compensation terms and the scope of services;

THEREFORE, the Parties wish to amend the Agreement to alter the scope of services and compensation terms.

This Amendment hereby removes Exhibit A and replaces it with the attached, updated Exhibit A.

All other provisions of the Agreement shall remain unchanged. This Amendment is the entire agreement of the patties regarding modifications of the Agreement provided herein, supersedes all prior agreements and understandings regarding such subject matter, may be modified only by a writing executed by the parties and their respective successors, legal representatives and assigns. The Agreement is ratified and confirmed in full force and effect in accordance with its terms, as amended hereby. In the event of any conflict between the te1ms of the Agreement and this Amendment, the provisions of this Amendment shall control.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment on the dates below to be effective as of July 18, 2024.

Jefferson County Public Schools:

By: .....
Dr. Martin A. Pollio
Superintendent

Date: _____

National Student Clearinghouse

By: Ricardo D Tones
Ricardo Tones
President & CEO

Date: 7/30/2024

Exhibit "A"

DESCRIPTION OF SERVICES

See StudentTracker for High Schools Agreement for Districts or High Schools between the Board and Service Provider, signed July 18, 2024, for a description of the services to be provided.

COMPENSATION

In consideration of the services provided by the Clearinghouse under this Agreement, JCPS agrees to pay the Clearinghouse a fee in accordance with the Clearinghouse's then-current Schedule of Fees for Secondary Schools. The current Schedule of Fees is below.

NATIONAL STUDENT CLEARINGHOUSE
SCHEDULE OF FEES FOR SECONDARY SCHOOLS
Published July 15, 2024 and Effective Until Further Notice

High schools, high school consortiums and/or high school districts ("programs") will pay an annual subscription fee for participation in the StudentTracker for High Schools program equal to $595.00 per participating high school.

The services will be provided at **no charge** to high schools that meet the following criteria:

- Have a total enrollment of less than 200 students; **AND**
- Are located in a district where four or more high schools pay the full annual StudentTracker for High Schools subscription fee.

StudentTracker® for High Schools Agreement (School, District, or Consortium)

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the National Student Clearinghouse ("Clearinghouse"), a not-for-profit corporation organized under the laws of the Commonwealth of Virginia, and the undersigned high school, high school district, or consortium ("School") agree as follows (the "Agreement"):

NATIONAL STUDENT CLEARINGHOUSE

Ricardo Torres
Signature

Ricardo D. Torres
Print Name

President
Title

7/18/2024
Date

www.studentclearinghouse.org

Email: contracts@studentclearinghouse.org

Jefferson County Public Schools
Name of School, District or Consortium

Dr. Dena Dossett 7/17/2024
Signature Date

Dr. Dena Dossett
Print Name

Chief of Accountability
Title (legal notices will be sent to this individual)

3332 Newburg Road
Street Address

Louisville, KY 40218
City/State/Zip

1-502-485-3036
Telephone

dena.dossett@jefferson.kyschools.us
Email

Contract Type:

☐ Single High School – account resides at the high school level

☒ School District – full or partial traditional school district

☐ Consortium of Schools –a group of schools from various locations, cities, states, etc.

The terms of this agreement incorporate Paragraphs 1 through 26 below and all attachments.

StudentTracker® for High Schools Agreement (School, District, or Consortium)

1. The Clearinghouse provides a nationwide, central repository of information on student enrollment, degrees, diplomas, certificates and other educational achievements.

2. The School wants to obtain information on the attendance of its former students in postsecondary institutions. The School wants to use the services of the Clearinghouse to evaluate the School's programs, improve instruction, and assist in the functions as described below and in the Attachments added hereto and made part hereof. School's research will be ongoing in order to provide a longitudinal study on student outcomes. Individual attachments may be added, deleted or modified by mutual written agreement.

3. The School will transmit to the Clearinghouse lists of its graduates ("Graduate File"). Initially, it will transmit a Graduate File dating back up to at least eight (8) years and, thereafter, will submit lists of new graduates each year after conferral of diplomas. The School agrees that it will submit its Graduates Files electronically and that they will contain the data elements and configuration reasonably required by the Clearinghouse.

4. The School shall ensure the Clearinghouse's performance of the Services meet the criteria of School Official set forth in the Schools annual notification of FERPA rights, unless another valid FERPA exception applies that permits the disclosure of Education Records by the School to the Clearinghouse. In its appointment as a School Official, the Clearinghouse shall be under the direct control of the School with respect to its use and maintenance of Education Records provided by the School. "School Official" means a contractor, consultant, volunteer, or other party to whom the School has outsourced school services or functions provided that they are performing a School service or function for which the School would otherwise use employees and is under the direct control of the School with respect to the use and maintenance of Education Records.

5. The School will institute and maintain reasonable controls to ensure that the information it provides to the Clearinghouse under this Agreement is complete and accurate. If the School learns of any inaccuracy or omission in the information in the Clearinghouse's possession, it shall promptly notify the Clearinghouse of such inaccurate or omitted information and provide a correction to such information. This includes promptly notifying the Clearinghouse of which students have chosen to block the release of directory information under FERPA.

6. Upon request, and at scheduled intervals, the Clearinghouse will compare the School's Graduate Files with its database and provide the School with data on the subsequent enrollment and educational achievements of its students at postsecondary institutions. In addition to the Graduate Files, the School may also submit lists of graduates and other former students in a format reasonably required by the Clearinghouse ("StudentTracker Request Files"), and the Clearinghouse will provide data on the subsequent enrollment and educational achievements of these students at postsecondary institutions.

7. School represents that it has signing authority for its participating educational entities, and that it is signing on behalf of the educational entities listed as Participating High Schools in Attachment 1 to this Agreement.

8. Both parties acknowledge that the security of the information exchanged is of critical importance. Both parties will comply with all applicable laws and regulations concerning the security and dissemination of the information exchanged hereunder including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA") and related federal regulations, and any applicable state laws concerning the privacy and security of the information to be shared hereunder.

   Institution will maintain appropriate security policies and procedures concerning the access of its staff to the secure areas of the Clearinghouse website or systems (which are at a minimum password-protected). The School is solely responsible for its compliance with FERPA, and the Clearinghouse is not liable for any errors or omissions by the School that may give rise to FERPA violations.

In the event either party determines that an event has occurred that reasonably leads it to believe that there has been an unauthorized or improper disclosure of the information exchanged under this Agreement, that party will promptly notify the other unless specifically directed not to make such notification by law enforcement. Such notification will include the nature of the incident, the information compromised, and the action taken. The parties will cooperate and keep each other informed until the incident is resolved. Either party shall have the right to immediately suspend service under this Agreement until the resolution of such incident.

9. In consideration of the services provided by the Clearinghouse under this Agreement, the School agrees to pay the Clearinghouse a fee in accordance with the Clearinghouse's published Schedule of Fees for Secondary Schools. The Clearinghouse is amending the fee schedule on July 15, 2024, and may additionally elect at any time after July 15, 2024 to amend such fee schedule by written notice to School no less than ninety (90) days prior to the effective date of such change. The School agrees to submit payment of applicable fees within thirty (30) days of receipt of an invoice from the Clearinghouse. If the School is a school district, it will submit a list of the names of the high schools covered by this Agreement on Attachment 1.

10. The School agrees that it may only disclose the data provided by the Clearinghouse to other educators, school boards and school officials whom it has determined to have legitimate educational interests. The School agrees that it will not release data provided by the Clearinghouse to any other individuals, institutions, or organizations, other than those identified above, either in student or postsecondary institution identifiable form, without the Clearinghouse's express written permission and payment of any additional fees that may be required.

11. In the event the School is required to disclose any data provided hereunder (specifically including, but not limited to, information which could potentially identify individuals or specific postsecondary institutions) pursuant to any applicable statute, law, rule or regulation of any governmental authority or pursuant to any order of any court of competent jurisdiction, the School must provide the Clearinghouse prompt notice of such request for disclosure and reasonably cooperate with the Clearinghouse's efforts to obtain a protective order. The parties further agree that any exclusion effected pursuant to this provision is authorized only to the minimum extent necessary to allow the School to comply with a legal rule or order compelling the disclosure of information and shall not constitute a general waiver of the obligations of confidentiality under this Agreement.

12. The School agrees to:
    a. Ensure that only authorized personnel whom it has determined to have legitimate educational interests will be provided with access to the Clearinghouse's secure website. School will notify the Clearinghouse immediately when personnel leave the School's employment, and the Clearinghouse will terminate such individual's access to the secure website.
    b. Take all necessary steps to ensure that authorized personnel do not share their Clearinghouse website user names and passwords with other individuals or entities.

13. The Clearinghouse will institute and maintain reasonable controls to ensure the integrity and security of its database and data transmission systems. Such controls will adhere to best practices and standards within the education community related to information security and will include technical, operational and physical controls which will be reflected in a comprehensive information security policy. The Clearinghouse will provide periodic security training to its employees who operate or have access to the database and data transmission systems. The Clearinghouse agrees to indemnify, defend, and hold the School harmless from and against any direct loss, cost, damage or expense suffered by the School as a direct result of the Clearinghouse's failure to comply with its obligations under this Agreement. The Clearinghouse will maintain insurance covering errors and omissions in its data processing operations in the amount of at least two million dollars ($2,000,000).

14. To the extent permitted by law, the School shall indemnify, defend, and hold harmless the Clearinghouse from and against any direct loss, liabilities, expenses, damages, or injuries (including, without limitation, all

maintain insurance covering errors and omissions in its data processing operations in the amount of at least two million dollars ($2,000,000).

14. To the extent permitted by law, the School shall indemnify, defend, and hold harmless the Clearinghouse from and against any direct loss, liabilities, expenses, damages, or injuries (including, without limitation, all costs and reasonable attorneys' fees) that the Clearinghouse may sustain arising out of or related to any third-party claim alleging: (1) a breach of this Agreement by the School or its Authorized Persons, (2) the Clearinghouse's use of incorrect or incomplete information received from the School, (3) the School's failure to notify the Clearinghouse of any suspected or actual unauthorized access to a password protected area of the Clearinghouse website, (4) any negligent or more culpable act or omission of the School or its Authorized Persons (including any reckless or willful misconduct) in connection with the performance of its obligations under this Agreement, or (5) any failure by the School or its Authorized Persons to comply with any applicable federal, state, or local laws, regulations, or codes in the performance of its obligations under this Agreement.

15. The School may audit at School's expense the performance by the Clearinghouse of its duties and obligations hereunder at the Clearinghouse offices during normal business hours but no more frequently than annually. Audits require 30 days advanced notice and will be scheduled at a mutually convenient date.

16. Nothing in this Agreement gives either party any rights in the intellectual property of the other including, but not limited to, copyrights, trademarks, patents and trade secrets. Neither party is granted a license in the intellectual property of the other, specifically including but not limited to trade secrets, patents, trademarks or copyrights. Upon termination of this Agreement, School will promptly discontinue use of any business methods, software or similar technology it may have acquired from the Clearinghouse during the term hereof. The Clearinghouse may develop, retain, or release aggregate or De-Identified data that does not contain Personally Identifiable Information which is in part comprised of information received from the School under this Agreement ("Reports"), subject to the ownership rights of School as set forth herein. The Clearinghouse owns all Reports generated under this Agreement, but its use of such Reports is limited as described in this Agreement.

    For purposes of this Agreement, the term "De-Identified" in reference to data shall mean that the data have undergone a process of removing the linkage between a set of identifying data and the individual to whom the data pertains.

17. Unless authorized under this Agreement or a subsequent amendment of the Agreement signed by the parties or by a signed and dated written consent of the student, the Clearinghouse shall not access, process, or disclose Education Records or Personally Identifiable Information received under this agreement for any purpose. As used in this Agreement the terms "Education Record" and "Personally Identifiable Information (or "PII") shall have the respective meanings below:

    "**Education Record**" has the meaning given to it by the Family Educational Rights and Privacy Act ("FERPA"), which covers records that are: (1) directly related to an enrolled or previously enrolled student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. Both the Graduate Files described in Section 4 and the Student Tracker Request Files described in Section 5 are Education Records.

    "**Personally Identifiable Information**" or "PII" means any information identified as personally identifiable information under FERPA or applicable state law.

    The Clearinghouse shall restrict access to Education Records and Personally Identifiable Information by its employees to those individuals that need to access the Education Records to facilitate performance by the Clearinghouse under the agreement and who are subject to a reasonable written non-disclosure agreement

with the Clearinghouse protecting the Education Records and Personally Identifiable Information, with confidentiality terms reasonably consistent with, and no less restrictive than, those found in this agreement.

Notwithstanding the forgoing, the Clearinghouse may release Graduation Information to the student about whom the information relates.

The Clearinghouse may use De-Identified data for purposes of research, the improvement of its products and services, and/or the development of new products and services that serve the learner, workforce and education communities in support of the Clearinghouse's mission. The Clearinghouse will take reasonable steps to ensure that all third-party recipients of De-Identified data will not re-identify or attempt to re-identify such De-Identified data. The Clearinghouse agrees that data provided by the School under this agreement may not be sold by the Clearinghouse, nor shall it be used by the Clearinghouse to amass a student profile for any purpose unrelated to the services provided pursuant to this Agreement, conduct targeted advertising, or market products or services.

18. Upon termination of this agreement, the Clearinghouse will immediately discontinue use of any information that has been provided to it by the School. The Clearinghouse agrees to destroy all information provided under this Agreement: (1) at the School's request; (2) when the data is no longer needed to achieve this Agreement's purposes, (3) upon termination of this Agreement, or (4) as otherwise required by state or federal law. School agrees that the Clearinghouse may maintain data provided by the School, when such data is needed to satisfy audit or other state and federal legal and regulatory requirements. Certification of this destruction will be at the School's request per the Clearinghouse's data deletion policy, or as otherwise may be required by the School.

19. The School agrees to acknowledge in all internal and external reports, presentations, publications, press releases, and/or research announcements that utilize StudentTracker data that the source of the data is the StudentTracker service from the Clearinghouse.

20. The School agrees to provide all notices to the Clearinghouse under this Agreement to:

    National Student Clearinghouse
    2300 Dulles Station Blvd., Suite 220
    Herndon, VA 20171
    Attn: Contracts Manager
    Electronically: contracts@studentclearinghouse.org

21. The Clearinghouse agrees to provide all notices in writing under this Agreement to the School to the signatory and address on Page 1 of this Agreement unless otherwise instructed in writing by the School. The Clearinghouse considers the signatory to this Agreement as its primary contact for all operational and systems issues unless otherwise instructed in writing by the School.

22. The effective date of this Agreement is the date by which it is signed by both parties. This Agreement will remain in effect until terminated by either party by providing sixty (60) days written notice to the other party. The parties agree that any subsequent modifications to this Agreement will be made only in writing. The Clearinghouse may assign this Agreement without consent to a successor or wholly owned subsidiary.

23. THE PARTIES AGREE THAT THE CLEARINGHOUSE IS NOT RESPONSIBLE FOR ANY ERRORS, ACTIONS, OR OMISSIONS BY THE SCHOOL. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR PUNITIVE DAMAGES UNDER THIS AGREEMENT OR IN CONNECTION WITH ANY SERVICES PROVIDED HEREUNDER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR SCHOOL'S MISUSE OF THE

SERVICES, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, PII, OR BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICES, DATA, OR ANY OTHER OUTPUT, EVEN IF THE CLEARINGHOUSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AVAILABLE REMEDIES ARE FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

THE PARTIES ACKNOWLEDGE THAT THE CLEARINGHOUSE HAS PROVIDED THE SERVICES AND EACH OF THE PARTIES HAS ENTERED INTO THIS AGREEMENT IN RELIANCE UPON THE LIMITATIONS OF LIABILITY AND THE DISCLAIMERS OF WARRANTIES AND DAMAGES SET FORTH HEREIN, AND THAT THE SAME FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES AND IN CONTEMPLATION OF CARRYING OUT THE PURPOSE OF THIS AGREEMENT BETWEEN THE PARTIES.

24. All representations, warranties, disclaimers of liabilities, indemnifications, and covenants between the parties will survive the termination of this Agreement for any reason and in any manner and will remain in full force and effect between the parties.

25. To the extent applicable under California law:

    a. Should an event rise to the level of a security breach, both parties to this Agreement shall reasonably cooperate together to fulfill either party's requirements under California data breach notification laws. The Clearinghouse shall follow its breach notification policy, which is in compliance with applicable federal and California laws. Notifications will include, written in plain language, the Clearinghouse's name and information about who to contact at the Clearinghouse, a list of the personal information we reasonably believe to have been the subject of a breach, a general description of the breach incident, and the steps we are taking to mitigate; and
    b. Except as otherwise provided in this Agreement, both parties agree that they may not disclose data obtained under this Agreement with any third party. Furthermore, both parties shall take all reasonable steps to ensure that third parties are prohibited from using identifiable information in Education Records to engage in targeted advertising.

26. Each party represents that the individual signing this Agreement on its behalf has the authority to do so and to so legally bind the party. The parties represent that the execution, delivery and performance of this Agreement has been fully and validly authorized.

27. Nothing in this Agreement gives either party any rights in the intellectual property of the other including, but not limited to, copyrights, trademarks, patents and trade secrets. Neither party is granted a license in the intellectual property of the other, specifically including but not limited to trade secrets, patents, trademarks or copyrights. Upon termination of this Agreement, School will promptly discontinue use of any business methods, software or similar technology it may have acquired from the Clearinghouse for use in performing the Service during the term hereof.

28. This Agreement and all related exhibits and Attachments, constitutes the sole and entire agreement of the parties to this Agreement with respect to the subject matter contained herein and therein, and supersedes all prior contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter.

29. No party shall be liable or responsible to the other party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control, including, without limitation: (a) acts of God; (b) flood, fire, earthquake, or explosion; (c) war, invasion, hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest; (d) government order or law; (e) actions, embargoes, or blockades in effect on or after the date of this

Agreement; (f) action by any governmental authority; (g) national or regional emergency (i) pandemic; and (j) shortage of adequate power or transportation facilities. The party suffering a Force Majeure Event shall give notice within 30 days of the Force Majeure Event to the other party stating the period of time the occurrence is expected to continue, and shall use diligent efforts to end the failure or delay and ensure the effects of such Force Majeure Event are minimized.

Attachment 1

StudentTracker® for High Schools Agreement

District Name	Jefferson County Public Schools
Date	8/21/2024

Participating High Schools

****PLEASE NOTE: Number of Enrollees refers to grades 9-12 only****

School Name:	**see Attachment 4 for list of schools** **City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**

ACT Code:
NCES Code:
Address:
Number of Enrollees:

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	

Address:
Number of Enrollees:

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

School Name:	**City, State:**
ACT Code:	
NCES Code:	
Address:	
Number of Enrollees:	

Attachment 2:
StudentTracker® for High Schools Agreement

NATIONAL STUDENT CLEARINGHOUSE
SCHEDULE OF FEES FOR SECONDARY SCHOOLS
Published July 15, 2024 and Effective Until Further Notice

High schools, high school consortiums and/or high school districts ("programs") will pay an annual subscription fee for participation in the StudentTracker for High Schools program equal to $595.00 per participating high school.

The services will be provided at **no charge** to high schools that meet the following criteria:

- Have a total enrollment of less than 200 students; **AND**
- Are located in a district where four or more high schools pay the full annual StudentTracker for High Schools subscription fee.

Attachment 3

STUDENTTRACKER® FOR HIGH SCHOOLS CONTACT LIST

School/District/Consortium Name:

*Executive Contact

(Primary point of contact other than signee)

Name: Tamara Lewis Title: Executive Administrator of Research and Systems Improvement

Email Address: tamara.lewis@jefferson.kyschools.us Phone Number: 1-502-485-3036

*Billing Contact

(Person to receive billing invoice)

Name: Tamara Lewis Title: Executive Administrator of Research and Systems Improvement

Billing Address: VanHoose Education Center, 3332 Newburg Road, Louisville, KY 40218

Email Address: tamara.lewis@jefferson.kyschools.us Phone Number: 1-502-485-3036

*Technical Contact(s)

(Person(s) responsible for creating, sending and receiving file data)

Name: Tamara Lewis Title: Executive Administrator of Research and Systems Improvement

Email Address: tamara.lewis@jefferson.kyschools.us Phone Number: 1-502-485-3036

Name: Ryan McCafferty Title: Specialist Accountability and Data Systems

Email Address: Ryan.mccafferty@jefferson.kyschools.us Phone Number: 1-502-485-3036

Name: _____ Title: _____

Email Address: _____ Phone Number: _____

Please email completed contract and attachments to: contracts@studentclearinghouse.org

Attachment 4

ACTCode	NCES	School Name	School Address	enrollment
181545	210299000632	Atherton High School	3000 Dundee Road Louisville, KY 40205	1473
181509	210299000695	Ballard High	6000 Brownsboro Road Louisville, KY 40222	2042
181512	210299000644	Butler Traditional High School	2222 Crums Lane Louisville, KY 40216	1366
181520	210299000730	Central High School	1130 W Chestnut Street Louisville, KY 40203	1165
181534	210299000691	Doss High	7601 St. Andrews Church Road Louisville, KY 40214	1152
181525	210299000734	Dupont Manual High	120 West Lee Street Louisville, KY 40208	1904
181810	210299000625	Eastern High	12400 Old Shelbyville Road Louisville, KY 40243	1826
180788	210299000651	Fairdale High School	1001 Fairdale Road Louisville, KY 40118	1418
180815	210299000628	Fern Creek Traditional High	9115 Fern Creek Road Louisville, KY 40291	1550
181543	210299000753	Iroquois High	4615 Taylor Blvd Louisville, KY 40215	1157
181513	210299002027	J Graham Brown School	546 S First Street Louisville, KY 40202	243
181292	210299000659	Jeffersontown High School	9600 Old Six Mile Lane Louisville, KY 40299	1054
181580	210299001705	Louisville Male High School	4409 Preston Highway Louisville, KY 40213	1853
181584	210299002026	Marion C Moore School	6415 Outer Loop Louisville, KY 40228	1180
182218	210299000668	Pleasure Ridge Park High	5901 Greenwood Road Louisville, KY 40258	1578
181612	210299000667	Seneca High	3510 Goldsmith Lane Louisville, KY 40220	1311
181620	210299000637	Southern High School	8620 Preston Highway Louisville, KY 40219	1570
181615	210299000777	The Academy @ Shawnee	4001 Herman Street Louisville, KY 40212	601
182575	210299000639	Valley High School	10200 Dixie Highway Louisville, KY 40272	848
181587	210299000649	Waggener High School	330 S. Hubbards Lane Louisville, KY 40207	902
181598	210299000677	Western High School	2501 Rockford Lane Louisville, KY 40216	506
A12977	210299000732	Binet School	3410 Bon Air Avenue Louisville, KY 40220	13
A12978	210299000789	Churchill Park School	435 Boxley Avenue Louisville, KY 40209	29
181581	210299001860	Mary Ryan Academy	3307 E Indian Trail Louisville, KY 40213	20
A13013	210299001447	Ahrens Educational Resource	546 South First Street Louisville, KY 40202	4
181514	210299001965	Breckinridge Metropolitan High	1128 East Broadway Louisville, KY 40204	121
180786	210299001612	Georgia Chaffee TAPP	1010 Neighborhood Place Louisville, KY	51

			40118	
181559	210299001634	Liberty High School	1281 Gilmore Ln Louisville, KY 40213	115
180017	210299002180	Newcomer Academy	3741 PULLIAM DR Louisville, KY 40218	456
181546	210299001947	Pathfinder School of Innovation	900 South Floyd Street Louisville, KY 40203	759
181644	210299002121	Phoenix School Of Discovery	502 WOOD RD Louisville, KY 40222	219
A12998	210299001935	U OF L Pact Program	102 Davidson Hall Room 102 Louisville, KY 40292	1
A12976	210299001859	Ackerly	200 East Chestnut Street Louisville, KY 40202	10
NULL	210299001943	Home Of The Innocents Discovery	1100 East Market Street Louisville, KY 40206	8
A12979	210299001946	Home Of The Innocents School	1100 East Market Street Louisville, KY 40206	22
181585	210299001492	Mary Jo and William MacDonald Maryhurst	1015 Dorsey Lane Louisville, KY 40223	39
181596	210299002412	Minor Daniels Academy	1960 Bashford Manor Lane Louisville, KY 40218	97
181603	210299001613	Peace Academy	2020 Newburg Road Louisville, KY 40205	55
A10161	210299001474	The Brook-KMI	8521 Lagrange Road Louisville, KY 40242	44

JEFFERSON COUNTY BOARD OF EDUCATION

Agenda for June 27, 2023, Regular Business Meeting

Agenda Item: **XI.R.19. Recommendation for Approval of a Data Privacy Agreement with National Student Clearinghouse**

Recommendation: Superintendent Martin Pollio recommends the Board of Education approve the attached Data Privacy Agreement with National Student Clearinghouse and authorize the superintendent to sign same.

Rationale: Jefferson County Public Schools (JCPS) uses the Student Tracker service from the National Student Clearinghouse to obtain accurate information on the educational outcomes of our graduates anywhere in the United States. Student Tracker covers more than 92 percent of all U.S. college enrollment.

Student Tracker provides the following information for JCPS high school graduates: college attendance, college enrollment, persistence in college, and degree attainment.

Submitted by: Dr. Dena Dossett

Attachment

OK AS TO FORM
A.M.H. 6/15/2023

This Confidential Data Privacy Agreement (**"DPA"**) is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the **"Board" or "Jefferson County Public Schools"**) and

NATIONAL STUDENT CLEARINGHOUSE, a non-profit business organized under the laws of Virginia with its principal place of business located at 2300 Dulles Station Blvd, Suite 220, Herndon, VA 20171 (the **"Provider"**).

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

WHEREAS, the Provider and the Board recognize the need to protect personally identifiable student infmmation 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 CPR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and the Board 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, the Board and Provider agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Entire Agreement.** This DPA sets out additional terms, requirements, and conditions on which the Service Provider will obtain, handle, process, disclose, transfer, or store Confidential Data when providing services under the Service Agreement This DPA may not be amended or modified except in writing as provided below.. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

2. **Term.** This DPA shall be effective as of June 28, 2023 (the **"Effective Date"**) and shall continue for three (3) years, terminating on June 27, 2026.

3. **Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit "A"** (the **"Services"**). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit "A"** (the **"Compensation"**).

4. **Purpose ofDPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Confidential Data including compliance with all applicable federal, state, and local privacy laws, rnles, and regulations, all as may be amended from time to time. In perfmming the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services othel wise provided by the Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Confidential Data.

5. **Confidential Data to Be Provided.** In order to perform the Services described above, the Board shall provide Confidential Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

6. **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 with respect to the interpretation of this DPA.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Confidential Data Property of the Board.** All Confidential Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the Board. The Provider further acknowledges and agrees that all copies of such Confidential Data transmitted to the Provider , are subject to the provisions of this DPA in the same manner as the original Confidential Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Confidential Data contemplated per the Service Agreement, shall remain the exclusive property of the Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Confidential Data, notwithstanding the above.

2. **Parent Access.** To the extent required by law the Board shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Confidential 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 the Board to respond to a parent or student, whichever is sooner) to the Board's request for Confidential 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 Confidential Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Board, 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 Board, transfer, or provide a mechanism for the Board 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 Confidential Data held by the Provider pursuant to the Services, the Provider shall notify the Board in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board 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 Confidential Data in a manner no less stringent than the terms of this DPA.

6. **Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff paiticipation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain pelmission from the Boai·d's IRB prior to beginning any research or evaluation related data collection.

ARTICLE III: DUTIES OF THE BOARD

1. **Provide Data in Compliance with Applicable Laws.** The Bomd shall provide Confidential 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 Board has a policy of disclosing Education Records and/or Confidential Data under FERPA (34 CFR § 99.3 l(a)(l)), the Board shall include a specification of criteria for detelmining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions.** The Board shall take reasonable precautions to secure usemames, passwords, and any other means of gaining access to the services and hosted Confidential Data.

4. **Unauthorized Access Notification.** The Board shall notify Provider promptly of any known unauthorized access. The Board will assist Provider in any effolts 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 peltaining to Confidential Data privacy and security, all as may be amended from time to time, 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 Infolmation 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. **Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designatedobelta Hyland as the data custodian ("Data Custodian") of the Confidential Data. The Board will release all data and information under this DPA to Data Custodian or to the Data Custodian's designated destination; provided, such destination is controlled by Provider. Data Custodian shall be responsible for Provider's compliance with the privacy and security terms of this DPA, including confirmation of the return or destruction of data as described below. The Board may,

upon request but no more frequently than annually, review the records Provider is required to keep under this DPA

3. **Authorized Use.** The Confidential 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 Provider will not contact the individuals included in the data sets without obtaining advance written authorization from the Board.

4. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Confidential Data to comply with all applicable provisions of this DPA with respect to the Confidential Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Confidential Data pursuant to the Service Agreement.

5. **Insurance.** Provider shall maintain, during the term of this Agreement, an errors & omissions policy with cyber liability coverage, with limits of no less than $5M aggregate. Upon request, Provider shall furnish the certificate of insurance evidencing this coverage. The ce1iificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate oflnsurance which shall read:

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

6. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Confidential Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Confidential Data other than as required by law or court order. If Provider becomes legally compelled to disclose any Confidential Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable effmis to provide the Board with prior notice before disclosure so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified infonnation or to Subprocessors perfmming services on behalf of the Provider pursuant to this DPA. Provider will not Sell Confidential Data to any third pmiy.

7. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Confidential Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Board 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 Leaming. Provider's use of De-Identified Data shall survive te1mination of this DPA or any request by the Board to destroy Confidential Data. Except for Subprocessors, Provider agrees not to transfer de-identified Confidential Data to any pmiy unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the Board who has provided prior written consent for such transfer. Prior to publishing

any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.

8. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of Confidential Data obtained under the Service Agreement in a usable fo1mat, within sixty (60) days of the date of said request and according to a schedule and procedure as the Patties may reasonably agree. Upon termination of this DPA Provider shall dispose of all Confidential Data. The duty to dispose of Confidential Data shall not extend to Confidential Data that had been De-Identified or placed in a separate student account pursuant to Alticle II, Section 3. The JCPS may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the JCPS and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Confidential Data described in **Exhibit "D"**.

9. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Confidential Data to (a) inf01m, 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 the Board. This section does not prohibit Provider from using Confidential Data (i) for adaptive Leaming or customized student Learning (including generating personalized Learning recommendations); or (ii) to make product recommendations to teachers or JCPS employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Data as permitted in this DPA and its accompanying exhibits.

10. **Liability.** Except to the extent caused by the negligence or willful misconduct of the Board or the Board's personnel or agents, Provider agrees to be responsible for and assumes all liability for any claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims"). Provider agrees to hold hatmless the Board and pay any costs incurred by the Board in connection with any Claim. The provisions of this Section shall survive the te1mination or expiration of this DPA.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Confidential Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Confidential Data is stored.

2. **Audits.** The Provider agrees and warrants that no more than once per year, upon request, it will make available to the LEA documentation sufficient to demonstrate that the Provider's processing of Student Data complies with security obligations required in this DPA. The LEA agrees to reasonably cooperate with the Provider to identify any particular documentation that may be reasonably required. Such documentation will include a copy of all third-patty certifications and/or audits (or auditor-prepared executive summaries thereof), in their then-most-current form, that relate to the Provider's compliance with data protection or information security standards or requirements. If the documentation provided by the Provider under this Section fails to demonstrate the Provider's compliance with any provision or aspect of applicable law and the LEA provides the Provider with detailed written notice of the same, the Provider shall submit its data files and documentation needed for processing the Student Data to reviewing, auditing, and/or certifying by the LEA (or any independent or impattial inspection, agents, or auditors bound by a duty of confidentiality, selected by the LEA and not reasonably

objected to by the Provider) to asceliain compliance with the wmTanties and undertakings in this DPA at a mutually agreeable time during regular business hours and upon no less than thiliy (30) days' prior written notice.

The LEA understands the Provider's documentation provided under this Section contains Confidential Information of the Provider, and it shall not disclose such documentation other than to its auditors and advisors and otherwise in compliance with the confidentiality obligations in this DPA and the Service Agreement in connection with verifying the Provider's compliance with the security and requirements in this DPA. If any audit or review referenced above uncovers deficiencies or identifies suggested changes in the Provider's provision of the Services, the Provider shall exercise reasonable efforts promptly to address such deficiencies and changes

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Confidential 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 an adequate Cybersecurity Framework based on one of the standards set fmih in **Exhibit "E"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "E"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:

   a) Encrypting all data, at rest and in transit;
   b) Maintaining multi-factor authentication on accounts that can access the network or email remotely, including 3rd party accounts;
   c) Securing access to any physical areas/electronic devices where sensitive data are stored;
   d) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
   e) Ensuring all staff and 3rd pmiies sign a nondisclosure statement, and maintaining copies of the signed statements;
   f) Installing end-point protection including but not limited to anti-malware and anti-spyware on any device connected to the network that has access to scoped data, when applicable

4. **Data Breach.** The Provider shall use reasonable efforts to immediately contain and remedy any Security Incident at the Provider's expense in accordance with applicable privacy rights, laws, regulations and standards. The Provider shall notify the LEA without undue delay but in any event no later than five calendar days from the Provider confirming a Security Incident, providing the LEA with sufficient information to allow the LEA to meet any obligations to report or inform data subjects of the Security Incident under applicable privacy and security laws and regulations. Such notification shall at a minimum:

   describe the nature and scope of the Security Incident, including the categories and numbers of data subjects concerned, the date of the Security Incident and the date of discovery of the Security Incident;
   communicate the name and contact details of the Provider's data protection officer or other relevant contact from whom more infmmation may be

obtained; and
describe the measures taken or proposed to be taken to address the Security Incident.

The Provider shall immediately take action to contain such Security Incident and mitigate potential risks to affected data subjects. The Provider may not disclose to any third party (except as legally required) whether Student Data was involved in any Security Incident unless and until expressly instructed to do so by the LEA. To the extent the Provider finds it is not feasible to provide the LEA with all the information described in this Section at the same time, the Provider may provide such info1mation to the LEA in phases to avoid any delay. The Provider shall not otherwise umeasonably withhold or delay its notification under this Section.

5. **Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.** If 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"), Provider shall secure, protect and maintain the confidentiality of the Personal Infimmation by, without limitation, complying with all requirements applicable to "non-affiliated third paiiies" 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 (I) 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;

11. A Social Security number;

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

1v. 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

v1. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Po1iability and Accountability Act), except for education records covered by FERPA.

b. As provided in KRS 61.931(5), a "non-affiliated third pmiy" 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. Provider shall not re-disclose, without the written consent of JCPS, any "personal infimmation, " as defined in KRS 61.931, or any other personally identifiable infimmation of a student or other persons, such as employees.

d. Provider agrees to cooperate, to the extent required by the Act or by this DPA, with JCPS in complying with the response, mitigation, conection, investigation, and notification requirements of the Act.

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

6. **Cloud Computing Service Providers.** If Provider is a cloud computing service provider (as defined in KRS 365.734(l)(b) as "any person other than an educational institution that operates a cloud computing service"), Provider agrees that:

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. Provider shall work with the student's school and district to detelmine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

Pursuant to KRS 365.734(2), Provider shall not in any case process student data to adveliise or facilitate advertising or to create or conect an individual or household profile for any adveliisement purposes.

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

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

ARTICLE VI: MISCELLANEOUS

1. **Termination.** This DPA will remain in full force and effect so long as (i) the Service Agreement remains in effect or (ii) the Provider retains any Confidential Data related to the Service Agreement in its possession or control. Either party may terminate this DPA if the other paiiy breaches any terms of this DPA, provided however, the breaching party shall have thirty (30) days to cure such breach and this DPA shall remain in force. Either Party may terminate this DPA in whole or in paii at any time by giving written notice to Provider of such termination and specifying the effective date thereof, at least thirty (30) days before the specified effective date. In accordance with **Attachment A,** the Board shall compensate Provider for Services satisfactorily performed through the effective date of termination.

2. **Effect of Termination Survival.** If the Service Agreement is telminated, the Provider shall destroy all of JCPS's Confidential Data pursuant to Aliicle IV, section 6.

3. **Priority of Agreements.** This DPA shall govern the treatment of Confidential Data 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, Telms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the teims of this DPA shall apply and take precedence.

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

5. **Disputes.** Any differences or disagreements arising between the parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.

6. **Notices.** All notices or other communication required or pelmitted to be given hereunder may be given via e-mail transmission, or certified mail, sent to the designated representatives below.

   The designated representative for the Board for this DPA is:

   Name: Tamara Lewis Title: Executive Administrator of Research and Systems Improvement

   Address: 3332 Newburg Road, Louisville, KY 40218

   Phone: 502-485-3036 Email: tamara.lewis@jefferson.kyschools.us

   The designated representative for the Provider for this DPA is:

   Name: Contracts Title: .....

   Address: 2300 Dulles Station Blvd, Suite 220, Herndon, VA 20171

   Phone: 703-742-4458 Email: Contracts@studentclearinghouse.org

7. **Amendment and Waiver.** 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 nanowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Pmiies, it shall, as to such jurisdiction, be so nanowly 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 COMMONWEALTH OF KENTUCKY, 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 JEFFERSON COUNTY KENTUCKY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

10. **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 telm of this DPA, the Provider shall provide written notice to the Board 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 Confidential Data within the Service Agreement. The Board 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.

11. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Confidential Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Confidential Data and/or any portion thereof.

12. **Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Provider. Neither Provider nor the Board 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.

13. **Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Oppoliunity Clause set folih in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.

14. **Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or pmiicipate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.

15. Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.

16. **Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: _____ Date: 6/27/23

Printed Name: Dr. Marty Pollio

Title/Position: Superintendent

NATIONAL STUDENT CLEARINGHOUSE

By: Ricardo Torres Date: 6/14/2023

Printed Name: Ricardo Torres

Title/Position: President & CEO

EXHIBIT "A"

DESCRIPTION OF SERVICES

~~See StudentTracker for High Schools Agreement for Districts or High Schools between the Board and Service Provider, signed August 5, 2019, for a description of the services to be provided.~~

COMPENSATION

~~Funds for purchase shall come from account code EV11217-0322-900XS. Total payments under this DPA shall not exceed $12,495.00 per fiscal year, running from July 1-June 30.~~

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	☐

6.7.2023 - NATIONAL STUDENT CLEARING HOUSE (FROM TAMARA LEWIS)

	Student class attendance data	☐
Communications	Online communications captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☑
	Place of Birth	☐
	Gender	☑
	Ethnicity or race	☑
	Language information (native, or primary language spoken by student)	☐
	Student disability information	☑

Category of Data	Elements	Check If Used by Your System
	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	☐
Schedule	Student scheduled courses	☐
	Teacher names	☐
Special Indicator	English language Learner information	☑
	Low income status	☑
	Medical alerts/ health data	☐

Category of Data	Elements	Check if Used by Your System
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Staff Data	First and Last Name	☐
	Email Address	☐
	Staff ID number	☐
	Other Information – Please specify	☐
Student Contact Information	Address	☐
	Email	☐
	Phone	☐

Student Identifiers	Local (School district) ID number	☐
	State ID number	☑
	Provider/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 student work data -Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐

	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: Diploma Type	☑
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

Compensation: Amounts to be paid to the Provider in exchange for services, software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider's standard pricing for that product.

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 infinmation 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 paiiy, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available info1mation.

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 the Board to provide a service to the Board shall be considered an "operator" for the purposes of this section.

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

Regulations: The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

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 Confidential Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a)

Security Incident: means any unauthorized access to, inadvertent disclosure of, or misuse of Confidential Data while in the possession or control of the Provider.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Confidential Data: Confidential Data includes any data, provided by the Board or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, info1mation in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other inf01mation allowing physical or online contact, discipline rccords, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic inf01mation, individual purchasing behavior or preferences, food purchases, political affiliations, religious inf01mation, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation inf01mation, parents' names, or any other information or identification number that would provide inf01mation about a specific student. Confidential Data includes Meta Data. Confidential Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Confidential Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Confidential Data as specified in **Exhibit "B"** is confitmed to be collected or processed by the Provider pursuant to the Services. Confidential 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.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes refened to as the "Subcontractor") means a party other than Board 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 Confidential Data.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Confidential Data or infened 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 adve1iisements. "Targeted Adve1iising" 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 Confidential 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

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board and Provider. The te1ms of the Disposition are set forth below:

.L Extent of Disposition

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

[Insert categories of data here]

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

£ 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:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

__ As soon as commercially practicable.

__ By **[Insert Date]**

Signature

_____ _____

Authorized Representative of the Board Date

Verification of Disn_osition of Data

_____ _____

Authorized Representative of Provider Date

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
X	American Institute of CPAs	SOC2
	International Standards Organization (ISO)	Information technology Security techniques - Information security management systems (ISO 27000 series)
	The Board of Education of Jefferson County	Board provided standardized questionnaire

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 08/30/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER MARSH USA INC. 1050 CONNECTICUT AVENUE, SUITE 700 WASHINGTON, DC 20036-5386 CN101455425-Prof.-D&O-22-23	CONTACT NAME: PHONE (A/C, No, Ext): FAX (A/C, No): E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : American Casualty Company Of Reading, Pa	20427
INSURED National Student Clearinghouse 2300 Dulles Station Boulevard, Suite 220 Herndon, VA 22071	INSURER B : Continental Casualty Company	20443
	INSURER C : Continental Insurance Company	35289
	INSURER D : Columbia Casualty Company	31127
	INSURER E :	
	INSURER F :	

COVERAGES CERTIFICATE NUMBER: CLE-006496365-16 REVISION NUMBER: 19

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS		
A	X COMMERCIAL GENERAL LIABILITY			6072191399	09/01/2022	09/01/2023	EACH OCCURRENCE	$	1,000,000
	CLAIMS-MADE X OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$	1,000,000
							MED EXP (Any one person)	$	15,000
							PERSONAL & ADV INJURY	$	1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$	2,000,000
	X POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$	2,000,000
	OTHER:							$	
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$	
	ANY AUTO						BODILY INJURY (Per person)	$	
	OWNED AUTOS ONLY / SCHEDULED AUTOS						BODILY INJURY (Per accident)	$	
	HIRED AUTOS ONLY / NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$	
								$	
C	X UMBRELLA LIAB X OCCUR			6072191354	09/01/2022	09/01/2023	EACH OCCURRENCE	$	5,000,000
	EXCESS LIAB CLAIMS-MADE						AGGREGATE	$	5,000,000
	DED RETENTION $							$	
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY			6072191368 (AOS)	09/01/2022	09/01/2023	X PER STATUTE OTH-ER		
B	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y/N: N	N/A		6072191371 (CA)	09/01/2022	09/01/2023	E.L. EACH ACCIDENT	$	1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$	1,000,000
							E.L. DISEASE - POLICY LIMIT	$	1,000,000
D	Cyber E&O			652260516	09/01/2022	09/01/2023	SIR: $150,000		10,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Board of Education of Jefferson County is additional insured for Cyber where required by written contract.

CERTIFICATE HOLDER	CANCELLATION
Board of Education of Jefferson County ATTN: Insurance/Real Estate Dept. 3332 Newburg Road Louisville, KY 40218	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE Marsh USA Inc.