

Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

NCS Pearson, Inc.

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 NCS Pearson, Inc., a corporation organized under the laws of Minnesota. ("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 July 28, 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 July 28, 2021: for the provision of Services Provider's products known as *Digital Assessment Library for Schools: Complete through Q-global and Q-interactive*, plus will also provide free record forms/response booklets for several other Pearson Clinical Assessments at no charge. These assessments include: KABC-II, KBIT-2, WASI-II, WNV, DAS-II, WRIT, WRMT-III, PAL-II, NEPSY-II, DKEFS, WRAML, PLS-5, CELF-5 Metalinguistics, Beery VMI, and BOT-2.
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 ("PII data") 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 PII 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 PII data 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 PII data necessary for the services or any changes to the scope, purpose or duration of the services themselves. Any agreed upon changes to the PII 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 PII data between each other. Services Provider shall confirm the transfer of confidential PII data and notify JCPS as soon as practicable of any discrepancies between the actual PII data transferred and the PII data described in this Agreement. The same protocol shall apply to any transfer of confidential PII data from Services Provider to JCPS.

C. CONSTRAINTS ON USE OF PII 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 PII data.
2. Services Provider will not contact the individuals included in the PII data sets without obtaining advance written authorization from JCPS.
3. Services Provider shall not re-disclose any individual-level PII data with or without identifying PII data to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS.
4. Services Provider shall use the PII data only for the purpose described in Paragraph B.1 above. The PII 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 PII data is confidential data and proprietary to JCPS, and agrees to protect the PII 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 PII 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 PII 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 PII 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 PII data.
 - d. Maintain any such PII data in a secure computer environment, and not copy, reproduce or transmit any such PII data except 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. Destroy or return to JCPS any such PII 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.
3. Services Provider shall not release or otherwise reveal, directly or indirectly, the PII 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 PII data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall 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 PII 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 PII 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 PII data.
5. Services Provider shall not use PII 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 PII 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 PII data to Services Provider.
6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the PII data do not gain access to the PII data. Reasonable security precautions and protections include, but are not limited to:
 - a. Creating, distributing, and implementing PII data governance policies and procedures which protect PII data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining PII data security;
 - b. Encrypting all PII data carried on mobile computers/devices owned by or under the control of Services Provider;
 - c. Encrypting PII data before it is transmitted electronically;
 - d. Requiring that users be uniquely identified and authenticated before accessing PII data;
 - e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the PII data necessary for this to perform their job functions;
 - f. Ensuring that all staff accessing PII data sign a nondisclosure statement, attached as **Attachment B**, and maintain copies of signed statements;

- c. 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 of any "Personal Information", as defined in KRS 61.931, 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 (as defined in KRS Chapter 365) 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 (as defined in KRS Chapter 365) 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 (as defined in KRS Chapter 365) 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 PII 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. JCPS may at any time destroy any or all of the PII data hosted on the Services Provider's Q-global™ and Q-interactive™ servers with Amazon Web Services. At any time (including upon termination of this Agreement), upon written request from JCPS, Services Provider shall securely and permanently destroy the PII data in the possession of Services Provider, 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 PII data to comply with this provision. Services Provider agrees to document the methods used to destroy the PII data, and upon request, provide certification to JCPS that the PII 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 Ian Wright at Ian.Wright@pearson.com (or an alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the PII data that JCPS shares with Services Provider. JCPS will release all PII data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all PII data requests and maintain a log or other record of all PII data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the PII 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 \$5,000,000. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage, with a copy of Services Provider's blanket endorsement. The certificate of insurance shall name the Board of Education of Jefferson County as additional certificate holder 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 PII data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student PII data requested under this agreement and costs associated with the electronic delivery of the student PII 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 PII data described in **Attachment A**.

G. LIABILITY

Services 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 Services Provider's intentional or negligent release of personally identifiable student, or parent PII data ("Claim" or "Claims"). Services Provider agrees to hold harmless JCPS and pay any costs incurred by JCPS in connection with any Claim, provided that JCPS provides Services Provider with prompt notice of any such Claims, and Services Provider is afforded the opportunity to control the defense and the settlement of any such Claims.. 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 PII data in Service Provider's possession pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after receipt of written notice from JCPS, Services Provider shall return or destroy all confidential information and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the PII data pursuant to Paragraph D.11.

3. Destruction of the confidential PII data 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 PII 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. INTENTIONALLY OMITTED

L. BREACH OF DATA CONFIDENTIALITY

Services Provider acknowledges that the breach of this Agreement or any part thereof, 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.

M. 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.

N. 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.

O. 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.

P. 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.

Q. 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.

R. 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:

NCS Pearson Inc.
19500 Bulverde Road, Suite 201
San Antonio, TX 75259

BY: Arthur Valh

Name: Arthur Valentine

Title: Managing Director for Clinical Assessment,
a division of NCS Pearson, Inc.

Date: 7/9/2021

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

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.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify: Country; language	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input checked="" type="checkbox"/>
	Other assessment data-Please specify: Clinical/skills assessments	<input checked="" type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input checked="" type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input checked="" type="checkbox"/>
	Other demographic information-Please specify: Ethnicity, language and other demographic data are optional.	<input checked="" type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>Q-global Data Elements Name - User's name is required, examinee name is optional Address - Q-global never collects nor stores addresses for users or examinees Phone number(s) - User's phone number and account contact phone number, never for examinee Email address - required for users; optional for examinee - only used when sending an ROSA to an examinee Race Pearson qualification level - account owners etc. level is associated to the account Log in ID and password - username and password for users (password is encrypted), never for an examinee Examinee ID - only required if examinee name is not provided Date of birth - required for every examinee Gender - only required for some assessments if gender norms are applicable Race and ethnicity - only required for some assessments if ethnicity norms are applicable Hardness - optional for some assessments Home language - optional for some assessments Clinical history - optional Education history and issues - optional Work and employment status, history and issues - optional Health conditions - optional Modifications - optional Mental status - may be required for some assessments Family information and history - optional Living arrangements - optional Names of parents or guardians - if sending a parent rate form, then the parent name and email are required to send the remote on screen assessment Test results and raw scores - Q-global does not store scored data, only item entry/raw score entry are stored</p> <p>Q-interactive Data Elements: Name - User's name is required, examinee name is required but any alphanumeric data can be entered into the form Phone number(s) - User's phone number and account contact phone number, never for examinee Email address - required for users, not entered for examinees Log in ID and password - username and password for users (password is encrypted), never for an examinee Examinee ID - ID can be any alphanumeric string Date of birth - required for every examinee Gender - required for every examinee Race and ethnicity - optional for some assessments Hardness - optional for some assessments Home language - optional for some assessments Clinical history - optional Education history and issues - optional Work and employment status, history and issues - optional Health conditions - optional Modifications - optional Mental status - optional Family information and history - optional Living arrangements - optional Test results and raw scores - for all assessments</p>	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

Attachment B

SERVICE PROVIDER'S EMPLOYEE NONDISCLOSURE STATEMENT

I understand that the performance of my duties as an employee or contractor of NCS Pearson, Inc. ("Services Provider") involve a need to access and review confidential personally identifiable information from an education record of a student ("PII data") (information designated as confidential by the Jefferson County Board of Education), and that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under applicable federal and state law. By signing this statement, I agree to the following:

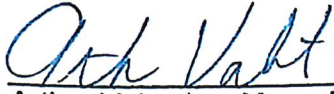
- I will not permit access to confidential PII data to persons not authorized by Services Provider.
- I will maintain the confidentiality of the PII data or information.
- I will not access PII data of persons related or known to me for personal reasons.
- I will report, immediately and within twenty-four (24) hours to my immediate supervisor, any known or reasonably believed instances of missing PII data, PII data that has been inappropriately shared, or PII data taken off site to my immediate supervisor.
- I understand that procedures must be in place for monitoring and protecting confidential PII data.
- I understand that the Family Educational Rights and Privacy Act ("FERPA") protects personally identifiable information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.

- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq) ("NSLA") or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.) ("CNA") and the regulations implementing these Acts, is confidential information.
 - I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the NSLA or the CNA and the regulations implementing these Acts, specifically 7 C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.
 - I understand that KRS 61.931 also defines "personal information" to include 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:
 - a) An account number, 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;
 - b) A Social Security number;
 - c) A taxpayer identification number that incorporates a Social Security number;
 - d) A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - e) A passport number or other identification number issued by the United States government; or
 - f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
 - I understand that other applicable federal and state privacy laws protect confidential PII data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that PII data as well.
 - I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, may be protected under applicable federal and state law.
- In addition, I understand that any data sets or output reports that I may generate using PII confidential data are to be protected. I will not distribute to any unauthorized person any data sets or reports that I have access to or may generate using confidential PII

data. I understand that I am responsible for any computer transactions performed as a result of access authorized by use of sign on/password(s).

Authorized
Employee signature:

Date:



7/9/2021

Arthur Valentine, Managing Director for
Clinical Assessment, a division of NCS Pearson, Inc.

61748842.2