OK AS TO FORM
FM 3-30-18

Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

International Data Evaluation Center

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 ("Data Provider") and the International Data Evaluation Center of The Ohio State University, Department of Teaching and Learning, College of Education and Human Ecology 1100 Kinnear Rd. Rm. 129, Columbus, Ohio 43212, Phone number, 614-429-1907 ("IDEC") describes the research project proposed by IDEC, and the means to be used by IDEC to ensure the confidentiality and security of information and data exchanged between Data Provider and IDEC.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of **April 25, 2018** and will terminate **June 30, 2020** unless terminated earlier by either party pursuant to Section H.

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

1. The International Data Center (IDEC), http://www.idecweb.us, is department of the College of Education and Human Ecology at The Ohio State University (hereinafter referred to as OSU). IDEC is responsible for collecting data for Reading Recovery in the United States. Reading Recovery is a short-term intervention for first graders. IDEC uses the data to create reports and data dumps that can be used by Reading Recovery stakeholders to evaluate the effectiveness of their respective Reading Recovery programs

   "Reading Recovery" is registered trademark owned by OSU. Every year OSU grants licenses to school districts to allow them to practice Reading Recovery, with the stipulation they will adhere to Reading Recovery's Standards and Guidelines. Part of those standards is to submit data to IDEC every year for analysis.

   IDEC is responsible for collecting data for Reading Recovery in the United States. IDEC uses the data to create reports and data dumps that can be used by Reading Recovery stakeholders to evaluate the effectiveness of their respective Reading Recovery programs. Most of said reports do not contain personally identifiable information, but some do, as identified in this Agreement. The description of which reports do and do not contain personally identifiable

information can be found in section **S** of this Agreement. The documents that do contain personally identifiable information are not released to the general public and are only accessible to the DATA PROVIDER's Reading Recovery Teacher Leader(s). IDEC also publishes a national report annually and will conduct its own internal research to examine trends in Reading Recovery. This national report will not contain personally identifiable student information; it will contain aggregate data only.

IDEC has its procedures annually reviewed by the Office of Responsible Research Practices at The Ohio State University. The consequence of not meeting their standards would result in the suspension of operations at IDEC until IDEC can meet their standards.

IDEC does not share data with any other entities.

IDEC analyzes data at the school and school district level using student data entered by Reading Recovery teachers, teacher data entered by Reading Recovery teachers, school data entered by Reading Recovery teachers and a control population of students; up to 10 students per school. The reports produced by IDEC contain both outcome and process results. The results examine the overall literacy progress of the children served, characteristics of the children being served, characteristics of teachers participating in Reading Recovery, and characteristics of schools participating in Reading Recovery. IDEC does not need direct access to DATA PROVIDER computers systems, classrooms, or children to facilitate its data collection.

2. Data Provider and IDEC agree that IDEC is an organization to which Data Provider can disclose, upon written request, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "studies exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(6) ("FERPA"), because the disclosure is to conduct studies for, or on behalf of, Data Provider to: develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

3. Data Provider shall disclose to IDEC, upon written request, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3, under the "studies exception" of FERPA, 34 C.F.R. 99.31 (a)(6), when the disclosure is to conduct studies for, or on behalf of, Data Provider to: develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. The confidential data including student and non-student information to be disclosed is described in a document attached to this agreement as **Attachment A.** IDEC shall use personally identifiable information from education records and other records in order to perform the studies described in Paragraph B.1 above. The description of the studies, as included in Attachment A, shall include the purpose and scope of the studies, the duration of the studies, a specific description of the methodology of disclosure

and an explanation as to the need for confidential data to perform these studies. IDEC shall notify Data Provider and Data Provider shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the studies or any changes to the scope, purpose or duration of the studies themselves. Any agreed upon changes to the data disclosed or to the studies shall be reduced to writing and included in Attachment A.

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

C. CONSTRAINTS ON USE OF DATA

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

2. IDEC will report only aggregate data and will not report any individual data, nor will data be reported in a manner that permits indirect identification of any individual.

3. IDEC will not contact the individuals included in the data sets without obtaining advance written authorization from Data Provider.

4. IDEC shall not re-disclose any individual – level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by Data Provider.

5. IDEC shall use the data only for the purpose described in Paragraph B.1 above. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

IDEC agrees to the following confidentiality and data security statements:

1. IDEC acknowledges that the data is confidential data and proprietary to Data Provider, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Data Provider, Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Privacy Act of 1974, 5 U.S.C. 552a;the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 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 Data Provider to IDEC of any data regarding any Data Provider student that is subject to FERPA, IDEC agrees to:

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

    b. Use any such data for no purpose other than to fulfill the purposes of the Project, and not share any such data with any person or entity other than IDEC and its employees, contractors and agents, without the approval of Data Provider.

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

    d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data expect as necessary to fulfill the purposes of the Project.

    e. Conduct the Project in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agent of IDEC having a legitimate interest in knowing such personal identification, and not disclose any such data in a manner that would permit the identification of an individual student in any published results of studies.

    f. Destroy or return to Data Provider any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by IDEC for the purposes of the Project.

3. IDEC shall not release or otherwise reveal, directly or indirectly, the data to any individual, Data Provider, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If IDEC becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then IDEC shall use all reasonable efforts to provide Data Provider with prior notice before disclosure so that Data Provider may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure Data Provider's compliance with the confidentiality requirements of federal or state law; provided, however, that IDEC will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, IDEC will only disclose that portion of confidential and otherwise personally identifiable data that IDEC is legally required to disclose.

4. IDEC shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data, other than publications permitted under Section I of this Agreement.

5. IDEC shall not use data shared under this Agreement for any purpose other than the goals outlined in this Agreement. Nothing in this Agreement shall be construed to authorize IDEC to have access to additional data from Data Provider that is not included in the scope of this Agreement (or addenda). IDEC understands that this Agreement does not convey ownership of the data to IDEC.

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

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

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

    c. Encrypting data before it is transmitted electronically;

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

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

    f. Ensuring that IDEC enforces the policies outlined in **Exhibit B.**

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

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

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

7. If IDEC 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"), IDEC shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

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

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

   ii. A Social Security number;

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

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

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

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

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

c. IDEC shall not re-disclose, without the written consent of Data Provider, 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. IDEC agrees to cooperate with Data Provider in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

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

8. IDEC shall report all known or suspected breaches of the data, in any format, to Dr. Dena Dossett, Chief, Data Management, Planning and Program Evaluation Division. 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 discover 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, or a breach of hard copies of records; (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.

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

10. For purposes of this agreement and ensuring IDEC's compliance with the terms of this Agreement and all application of the state and Federal laws, IDEC designates Jeff Brymer-Bashore as the temporary custodian ("Temporary Custodian") of the data that Data Provider shares with IDEC. Data Provider will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. Data Provider or its agents may, upon request, review the records IDEC is required to keep under this Agreement.

11. IDEC has the right, consistent with scientific standards, to present, publish, or use student results it has gained in the course of its analysis, but only if the publication, presentation, or use does not include personally identifiable information of parents, students, or teachers, and not outside the bounds of a research study.

12. Should IDEC use or collect data for the purpose of conducting a research study, IDEC will separately submit an external research request through Data Provider's online system: https://assessment.jefferson.kyschools.us/DRMS/.

13. Should IDEC publicly present, publish, or use student results that **solely** uses data from Data Provider, IDEC shall adhere to the following terms:

    a. IDEC shall not publish, present, or use reports that include a cell size of less than 10. Reports must mask these cells so that the results are not revealed.

    b. Publications and reports of data and information shared, including preliminary descriptions and draft reports, shall involve only

aggregate data and no personally identifiable information or other information that could lead to the identification of any student, parent, or teacher.

c. No less than fifteen (15) business days prior to public disclosure of its data analysis, IDEC will provide Data Provider a manuscript or other draft of the proposed public disclosure. Within fifteen (15) business days following receipt thereof, Data Provider will notify IDEC in writing if the proposed disclosure contains any confidential information and specify the portions of the proposed disclosure requiring redaction.

d. IDEC shall provide Data Provider, free of charge and within thirty (30) days, a copy of any report that is generated using the data.

e. Reports or articles based on data obtained from Data Provider under this agreement must include the following acknowledgment: "This report/article was made possible, in part, by the support of the Jefferson County, Kentucky, Public Schools. Opinions contained in this report/article reflect those of the author and do not necessarily reflect those of the Jefferson County, Kentucky, Public Schools." Data Provider must be cited as the source of the data in all tables, reports, presentations, and papers.

14. IDEC 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 Data Provider to immediately terminate this Agreement.

E. FINANCIAL COSTS OF DATA-SHARING

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

No payments will be made under this agreement by either party.

F. OBLIGATIONS OF DATA PROVIDER

During the term of this Agreement, Data Provider shall:

1. Prepare and deliver student demographic and academic data as defined in **Attachment A** – Data File Description. All items will be keyed to a "proxy" student identifier that is different from the official student ID. The link between the official and proxy IDs will not be disclosed by Data Provider. No personally identifiable information will be provided to IDEC.

2. After the initial data is provided for the requested student population, Data Provider will not provide supplementary data for additional students.

3. Provide Data Stewardship training for data custodian.

G. LIABILITY

Each Party to this Agreement shall be responsible for any liability, claim, loss, damage or expenses, including without limitation, reasonable attorney fees, arising from its negligent acts or omissions in connection with its performance of this Agreement, or its failure to comply with the terms of this Agreement, as determined by a court of competent jurisdiction, pursuant to Ohio Revised Code 2743.02.

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 immediately in the event of a material breach of this Agreement by another party.

    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, the confidential information shall be returned or destroyed within seven (7) days of the termination. If this Agreement terminates at the end of the term described in Section A, IDEC shall return or destroy all confidential information when it is no longer needed for the study. Such return or destruction shall occur within seven (7) days after it is no longer needed for the study.

3. Destruction of the confidential information shall be accomplished by utilizing an approved methods of confidential destruction, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer or researcher. If new materials are developed during the project, ownership and copyright of such will remain with the developing entity.

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. QUALITY OF SERVICES

Data Provider reserves the right to review IDEC's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1. Failure of IDEC to perform in a manner that meets or exceeds the quality standards for Data Provider shall serve as grounds for termination of this Agreement.

L. BREACH OF DATA CONFIDENTIALITY

IDEC acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to Data Provider for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by IDEC, Data Provider, in addition to any other rights and remedies available to Data Provider at law or in equity, may be entitled to seek 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 IDEC has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), Data Provider may not allow IDEC access to personally identifiable information from 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, except that any claims arising under federal law shall be governed and construed in accordance with federal law. Any action or claim against the Data Provider arising from, under or pursuant to this Agreement shall be brought in the Jefferson County, Kentucky, Circuit Court, and any action or claim against IDEC arising from, under or pursuant to this Agreement shall be brought in the Ohio Court of Claims pursuant to Ohio Revised Code 2743.02, 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 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

Data Provider is not an employee, agent, partner or co-venturer of or with IDEC. Neither IDEC nor Data Provider 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. IDEC shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of Data Provider, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

S. DESCRIPTION OF PRODUCTS PRODUCED BY IDEC

1. Annually, IDEC will provide the following to DATA PROVIDER Teacher Leaders or an employee designated by the Superintendent of DATA PROVIDER, via secure download from the IDEC web site.

a. If a teacher leader is employed by more than one school district, IDEC will produce a report that contains aggregate results for all those school districts. IDEC refers to this type of report as a site level report. This report is only available to the teacher leader and not available to the general public. This report will not contain personally identifiable student information; it will contain aggregate data only.

b. Student, School, and Teacher Data Dump – An excel spreadsheet that contains all data entered by DATA PROVIDER Reading Recovery teachers. This data dump will include contain personally identifiable student information.
c. School District Summary of Reading Recovery in DATA PROVIDER.

This report will not contain personally identifiable student information; it will contain aggregate data only.

d. One school report for each school participating in Reading Recovery in DATA PROVIDER. These summaries contain a mixture of aggregate results and results that contain personally identifiable information of both Reading Recovery Teachers and students. These summaries are not accessible to the general public and can only be accessed by a Reading Recovery Teacher Leader. Individual Reading Recovery teachers do not have access to the summary for the schools in which they work. The summaries contain a highly visible warning message like the example below:

WARNING

Please note students' names and demographic information are included in this data summary. It is highly confidential in nature. Do not distribute it to board members, PTOs or other unauthorized personnel.

The information in this document is confidential and may be subject to state and/or federal student privacy laws and/or local school district privacy policies. It is intended solely for the attention and use of authorized employees of [SCHOOL NAME]. If you are not an authorized employee of [SCHOOL NAME], or person responsible for delivering this document to an authorized employee, please notify your Reading Recovery Teacher Leader(s), [LIST OF TEACHER LEADERS], immediately.
Unless you are an authorized employee of [SCHOOL NAME] or his/her representative you are prohibited from, and therefore must not, read, copy, distribute, use or retain this document or any part of it.

AGREED:

FOR THE INTERNATIONAL DATA EVALUATION CENTER OF THE OHIO STATE UNIVERSITY, DEPARTMENT OF TEACHING AND LEARNING, COLLEGE OF EDUCATION AND HUMAN ECOLOGYIDEC1100 Kinnear Rd, Room 129
Columbus, OH 43212

Michael Papadakis

Michael Papadakis
Interim Sr. Vice President for Business and Finance and CFO/Treasurer

Ohio State University Date: 3-19-18

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: _____

Name: _____

Title: _____

Date: _____

61712202.1

ATTACHMENT A: SPECIFIC RECORDS OR DATA ELEMENTS

Reading Recovery Student Data

1. *Student Name*
2. *Student ID Number (Optional)*
3. *School*
4. *Gender*
5. *Date of Birth*
6. *[Data point removed by agreement of the parties. Space kept for consistency in numbering]*
7. *Native Language*
8. *Race/Ethnicity*
9. *Disability Status*
10. *Scores on a diagnostic tool called the Observation Survey/Instrumento de Observacion which is administered in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year, along with the dates the tool was administered.*
11. *Scores on a diagnostic tool called Slosson Oral Reading test which is administered in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year. (Optional)*
12. *Classroom literacy performance as compared to peers in the fall, at the start of child's intervention, at the end of the child's intervention, and at the end of the school year.*
13. *English Proficiency in the fall if the child is not a native English speaker*
14. *The date the child's intervention started and ended.*

15. *Whether or not the child successfully completed the intervention*

16. *Misc. comments about the child's intervention if their intervention was not successful.*

17. *The length of the child's intervention in weeks*

18. *The number of lessons a child received*

19. *The number of lessons the student missed*

To authorize the release and use of confidential data under the FERPA Studies Exception. Exhibits referenced in the Agreement must be completed and incorporated into the final Agreement.

Exhibits include:

- Exhibit A –
    - Section I - describes the study, funding source and data being requested
    - Section II- describes the need for Personally Identifiable Information (PII)
    - Section III required if requesting Free and Reduced Lunch information
- Exhibit B – IDEC Nondisclosure Statements
- Exhibit C – IDEC data security policy
- Exhibit D – Data destruction plan at completion of study and identification of data custodians
- Exhibit E — IDEC's Certificate of Data Destruction

Please refer to The U.S. Department of Education, Family Policy Compliance Office's Guidance for Reasonable Methods and Written Agreements *for additional information on requirements for data sharing under the Family Educational Rights and Privacy Act (FERPA).*

Contact Information:

Research Organization Legal Name: The Ohio State University, on behalf of the International Data Evaluation Center

Primary Data Custodian Name: Jeff Brymer-Bashore

Title: Director of IT and Operations

Phone: 614-360-1900 Email: brymer-bashore.1@osu.edu

Secondary Data Custodian Name:

Title:

Phone: Email:

Section I – to be completed by all requestors:

Describe purpose, scope and duration of study – *use of data received under this agreement is limited to purpose and scope defined.*

- Describe purpose and scope of the study.
  Reading Recovery (RR) is an early literacy intervention that serves first grade children who are struggling the most with literacy. The goal of RR is to bring those children up to average levels of literacy within 12 to 20 weeks. We collect data to provide annual evaluation reports to every school participating in Reading Recovery, conduct analysis at the national level for publication in journals, and create on-going professional development opportunities for Reading Recovery teachers and teacher leaders using national data.

- Describe any grant, third party or other funding source for study.
  We do not receive outside money for data collection. It is solely funded by the fees we charge the schools participating in Reading Recovery.

- Describe how results of study will be used and include Vision 2020 strategy supported by the study.
  One of the Strategies of Vision 2020 includes Improve Student Literacy (1.1.5). The results will be used as a data point to track progress towards ensuring ALL…

Start Date of Study: Reading Recovery has been collecting data since 1984 End Date of Study: There is not current end date for Reading Recovery.

Data Being Requested – provide specific data elements needed to complete study. – See attachment A.

Section II – Complete if Personally Identifiable Information (PII) is being requested:

- Justify your request for student/individual level data. – Part of the services we provide are creating school district and school level reports that teachers, principals, and school district administrators use evaluate the effectiveness of their Reading recovery implementation. This evaluation sometimes relies on being able to report back individual level student data to these stakeholders.

- Explain why study could not be completed using aggregate-level data without PII.-The services that you pay for, receiving personalized student, school, and school district reports, would not be possible to provide to you with the PII data.

Special requirements for requests for Personally Identifiable Information (PII)

- *Student-Level/Individual detail from education records can only be used to meet the purpose or purposes of the study as stated in this MOU for duration as defined.*
- *IDEC agrees to conduct the study in a manner that does not permit the personal identification of parents, students, individuals by anyone other than designated data custodians.*
- *IDEC agrees to destroy all PII from education records and confidential data from other records.*

If Free/Reduced Lunch status is needed on PII, complete Section III.

Though our data system asks for Free/Reduced status, it is not required and can be left blank by teachers. It is not needed for our research.

Section III

Complete if free or reduced -price lunch eligibility data is required for Project

Disclosure of Free and Reduced Price Information

A. Purpose and Scope

Jefferson County Public Schools, DATA PROVIDER, and IDEC___acknowledge and agree that children's free and reduced price meal and free milk eligibility information obtained under provisions of Richard B. Russell National School Lunch Act (42 USC 1751 et. seq.) (NSLA) or Child Nutrition Act of 1966 (42 USC 1771 et. seq.) (CNA) and the regulations implementing these Acts is confidential information. This Agreement is intended to ensure that any information disclosed by the DATA PROVIDER to _IDEC about children eligible for free and reduced price meals or free milk will be used only for purposes specified in this Agreement and that the DATA PROVIDER and ___IDEC____ recognize that there are penalties for unauthorized disclosures of this eligibility information.

B. Authority

Section 9(b) (6) (A) of the NSLA (42 USC 1758(b) (6) (A)) authorizes the limited disclosure of children's free and reduced price meal or free milk eligibility information to specific programs or individuals, without prior parent/guardian consent. Except that, the parent/guardian must be provided the opportunity to decline to share eligibility information prior to the disclosure for identifying children eligible for benefits under or enrolling children in the State Medicaid Program and the State children's health insurance program. Additionally, the statute specifies that for any disclosures not authorized by the statute, the consent of children's parents/guardians must be obtained prior to the disclosure.

The requesting DATA PROVIDER certifies that it is currently authorized to administer the following program(s) and that information requested will only be used by the program(s) indicated.

Check all that Apply	Program	Information Authorized

	Medicaid or the *State children's health insurance program (SCHIP),* administered by a State or local DATA PROVIDER authorized under titles XIX or XXI of the Social Security Act.	All eligibility information unless parents elect not to have information disclosed.
	State health program other than Medicaid/SCHIP, administered by a State DATA PROVIDER or local education DATA PROVIDER.	Eligibility status only; consent not required
	Federal health program other than Medicaid/SCHIP Specify Program:	No eligibility information unless parental consent is
	Local health program Specify Program:	No eligibility information unless parental consent is
	Child Nutrition Program under the National School Lunch Act or Child Nutrition Act	All eligibility information; consent not required.
	Federal education program Specify Program:	Eligibility status only; consent not required.
	State education program administered by a State DATA PROVIDER or local education DATA PROVIDER	Eligibility status only; consent not required.

Note: Section 9(b(6)(A) specifies that certain programs may receive children's eligibility status only, without parental consent. Parental consent must be obtained to disclose any additional eligibility information. Section 9(b)(6)(D)(ii) specifies that for State Medicaid or SCHIP, parents must be notified and given opportunity to elect not to have information disclosed. Social security numbers may only be disclosed if households are given notice of the disclosure and the uses to be made of their social security numbers as required by Sec. 7 of the Privacy Act.

C. **Responsibilities**

DATA PROVIDER will:

When required, secure parents/guardians consent prior to any disclosure not authorized by the National School Lunch Act or any regulations under that Act, unless prior consent is secured by the receiving DATA PROVIDER and made available to the determining DATA PROVIDER;For State Medicaid and SCHIP, notify parents/guardians of potential disclosures and provide opportunity for parents/guardians to elect not to have information disclosed; Disclose eligibility information only to persons directly connected to the administration or enforcement of programs authorized access under the National School Lunch Act or regulations under the Act or to programs or services for which parents/guardians gave consent.

IDEC will:

Ensure that only persons designated as data custodians and listed on Exhibit E who are directly connectedwith the administration or enforcement of the ___(program) and whose job responsibilities require use of the eligibility information will have access to children's eligibility information.

Use children's free and reduced price eligibility information for the following specific purpose(s):

Describe:

Inform all persons that have access to children's free and reduced price meal eligibility information that the information is confidential, that children's eligibility information must only be used for purposes specified above, and the penalties for unauthorized disclosures.

Protect the confidentiality of children's free and reduced price meal or free milk eligibility information as follows:

Specifically describe how the information will be protected from unauthorized uses and further disclosures:

Effective Date

This agreement shall be effective during the dates of duration for the study.

D. Penalties

Any person who publishes, divulges, discloses, or makes known in any manner, or to any extent not authorized by Federal law (Section 9(b)(6)(C) of the National School Lunch Act; 42 USC 1758(b)(6)(C)) or regulation, any information about a child's eligibility for free and reduced price meals or free milk shall be fined not more than a $1,000 or imprisonment of not more than 1 year or both.

E. Signatures

The parties acknowledge that children's free and reduced price meal and free milk eligibility information may be used only for the specific purposes stated above; that unauthorized use of free and reduced price meal and free milk information or further disclosure to other persons or programs is prohibited and a violation of Federal law which may result in civil and criminal penalties.

IDEC

Typed or Printed Name: _____

Title: _____Phone:

Signature: _____

Date: _____

Data Provider

Name:. _____

Title:_____Phone: _____

Signature: _____

Date:

**Any attachments will become part of this agreement.*

Exhibit B

IDEC NONDISCLOSURE STATEMENT

IDEC: International Data Evaluation Center on behalf of The Ohio State University

IDEC understands, that it is required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. IDEC will not permit access to confidential information to persons not authorized by the IDEC. IDEC will maintain the confidentiality of the data or information.

- IDEC employees will not access data of persons related or known for personal reasons.
- IDEC will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by IDEC or others for any purpose other than statistical purposes specified in the IDEC survey, project, or proposed research.
- IDEC will report, within forty-eight (48) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site to DATA PROVIDER
- IDEC understands that procedures must be in place for monitoring and protecting confidential information.
- IDEC understands that FERPA protects information in students' education records that are maintained by an educational DATA PROVIDER or institution or by a party acting for the DATA PROVIDER 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.
- IDEC understands 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.
- IDEC understands and acknowledges 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.
- IDEC understands 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 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, 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.

- IDEC understands 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 DATA PROVIDER;
e) A passport number or other identification number issued by the United States government; or
0 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.

- IDEC understands that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- IDEC understands that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

In addition, IDEC understands that any data sets or output reports that it may generate using confidential data are to be protected. IDEC will not distribute to any unauthorized person any data sets or reports that IDEC has access to or may generate using confidential data. IDEC understand that IDEC am responsible for any computer transactions performed as a result of access authorized by use of sign on/password(s).

Exhibit C

Please describe the measures you take to ensure the protection of data released to you. If you have a policy, please attach or copy/paste here as Exhibit C and include information on the requested delivery method.

IDEC's data systems are stored at the College Of Education and Human Ecology's data center located at the State of Ohio Data Center. Access to this building is controlled by two-factor authentication. To enter and move around inside the building one must have an access card to open a door. This includes the doors on the outside of building. Once a card is swiped, the person holding the card must enter a PIN number as the second part of the authentication process. If the PIN is incorrect, the door will not open. The servers that run our data systems are stored in a locked cage that can only be accessed using this 2-factor authentication of swiping a card and supplying a PIN number. A security guard is also present watching the front doors. Data systems are also protected from electronic intrusion by a network firewall.

As the stewards of Reading Recovery data, it is important that IDEC deliver information to our stakeholders and interested parties as efficiently as possible while enforcing appropriate data security practices. In most cases, the roles and relationships within Reading Recovery clearly dictate who is allowed access to what type of data. At other times, it is not quite as clear about who is entitled or not entitled to receive data. In these scenarios IDEC assumes a role of neutrality in the decision making process and falls back on our protocol of the certifying authority.

Being an entity at The Ohio State University IDEC is held to strict data privacy standards and all the research data collected by IDEC is classified by the institution as S3 data, or private data. IDEC is reviewed annually by Ohio State's Office of Research to make sure that we are taking precautions to protect the data that is being housed in our data systems. When a

request for data comes to IDEC, employees follow strict procedures to determine whether or not the requesting party is eligible to have de-identified data. If applicable, IDEC will instruct data requesters to contact the school district that owns the data for permission.

Teacher will enter data using the IDEC web site. Every teacher is issued a unique username and password and can only see the data entered by them. Our web sites use 256-bit SSL (Secure Sockets Layer) encryption to protect data as it is being entered by teachers.

Exhibit D

When it becomes necessary to permanently destroy data, IDEC will do following to sanitize it systems of DATA PROVIDER's data:

1. IDEC will perform a DELETE T-SQL command to delete all student, teacher and school data from IDEC database management system.
2. Our database management system keeps 3-days of backups locally, it will take 3 days for DATA PROVIDER's data to be purged from local backups
3. Additionally, IDEC stores 30 days of automated backups off-site and it will take any additional 30 days for data to be purged from off-site automated backups.
4. Reports and data dumps that were available for teacher leaders to download from our web site are stored in cloud-based file storage system. IDEC will delete these files using the cloud-storage's built-in delete functionality. The cloud-storage keeps these files for 30 days and then permanently deletes them. DATA PROVIDER's will be permanently deleted after 30 days.

Primary Data Custodian

Last Name, First Name:Brymer-bashore, Jeff_____Last Name, First Name: __

Phone: 614-360-1900_____Phone:____

Email: brymerj@idecweb.us_____ Email:____

Employer: The Ohio State University _____ Employer: ___

Exhibit E

IDEC'S CERTIFICATE OF DATA DESTRUCTION

The IDEC shall irreversibly destroy all copies of all confidential and otherwise personally identifiable data regardless of format (e.g. paper, electronic) within forty-five (45) days after it is no longer needed to perform the studies described in this agreement, upon DATA PROVIDER's request or upon termination of this agreement, whichever occurs first unless agreed otherwise in writing. Using this form, the IDEC shall provide written verification of the data destruction to the DATA PROVIDER within forty-five (45) days after the data is destroyed. Scan the signed Certificate of Data Destruction and return it to
.

If the IDEC uses a contractor for data destruction services, a certificate of destruction from the contractor is also required. Please submit the contractor's certificate of destruction with this signed Certificate of Data Destruction.

In accord with the provisions of the DATA SHARING AGREEMENT between the Data Provider and the ("IDEC" or "Contractor"), the confidential and otherwise personally identifiable data were destroyed as required in Section N according to the methods described in Exhibit D of the DATA SHARING AGREEMENT.

Date submitted:

Scheduled date of destruction (per DATA SHARING AGREEMENT):

Actual destruction date:

Media	Method of Destruction	Comments

I hereby certify that all confidential and otherwise personally identifiable data described above have been destroyed in the manner indicated.

IDEC's Authorized Agent Signature / Date

Agent's Name: **Agent's Title:**

Data Breach Mitigation Policy

Purpose

This section describes the actions that need to be taken in the event that data are stolen from IDEC. This policy does not cover the accidental release of data by an IDEC employee. Those should be handled on a case-by-case IDEC's Directors of IT and Operations. He / She will choose the appropriate course of action to handle the matter.

Description

The following will actions will take place in the event of data breach

1. Notifications process
    a. Notify IDEC's Director of Research
    b. Notify Office Responsible Practices, done by Director of Research
    c. Notify Office of Information Technology for the College of Education
    d. If appropriate, notify proper Authorities
    e. Gather Description of Event
    f. Identify Location of Event
2. Investigation Steps
    a. Establish a response team (Director of IT and Op; Systems Manager, Director of Research)
    b. Identify and take immediate action to stop the source of the attack or entity responsible
    c. Determine and notify key stakeholder (ie TLs, Trainers, Principals, etc..). Director of Research will determine who to notify with help of IDEC staff.
    d. Identify source or suspects of the event
    e. Carry out IT forensics investigation to gather evidence
    f. Determine need for external law enforcement
    g. Determine to contact other additional stakeholders
3. Other Actions if Applicable
    a. Contact law enforcement
    b. Collection of evidence
    c. Notification of victims
    d. Prepare written communication plan to cover oral and written communication to parties involved
    e. Communication with media
4. Follow-up activities
    a. Evaluation of Security Incident Response
    b. Determine
        i. How well did the work force members respond to event?
        ii. Were documented procedures followed? Were they adequate?
        iii. What information was needed sooner?
        iv. Were there any steps or actions that might have inhibited recovery?

v. What could work force members do differently the next time an incident occurs?
vi. What corrective actions can prevent similar events in the future?
vii. What additional resources are needed to detect, analyze, and mitigate future incidents?
viii. What external resources and contacts proved helpful?
ix. Other conclusions or recommendations