

OLA General Contract Entry Form

Agreement Name *

IDEC – Steven Point FY22–24 Data Privacy Agreement

Full Legal Name of Other Party *

Steven Point Area Public School District

Term of Contract Start *

12/20/2021

Term of Contract End *

06/30/2024

Originator *

PRUCHNICKI.3

General Contract Reviewing Attorney *

beerck.1

CM D–Org *

D1275

Amount *

\$0.00

Business Purpose *

Define standards for use of data for analysis and eval services provided by IDEC to SPAPSD.

Handling Instructions

Will Protected Health Information (PHI) be disclosed by either party pursuant to this agreement? *

No

Is a bid waiver required? (if so, please attach) *

No

Is this an amendment to a current contract? *

No

Upload General Contract (1)

CM General Contract *

[CM General Contract LAC# 220433 | IDEC – Steven Point FY22–24 Data Privacy Agreement for \\$0.00 | Steven Point Area Public School District | PRUCHNICKI.3 | beerck.1](#)

Upload Additional Back–up Documentation (0)

CM Back–up Documentation

Please confirm the following:

- I have reviewed this contract with the appropriate Department Approval Individual set forth above, and that individual is aware of the contract and all terms therein, and has approved same. *
- The contract was reviewed by a member of The Office of Legal Affairs and I received permission to upload the document into OnBase. I certify that the document attached is the final approved version of the document. *
- The contract and all necessary exhibits are attached. *
- I have read the contract in its entirety and believe it reflects the business terms negotiated between the parties. *



Initiator	<p>Notify Fiscal Officer via email of the need to route a contract for review in a timely fashion and inform FO of all necessary deadlines well in advance.</p> <p>Provide a copy of the contract to the Fiscal Officer.</p> <p>Complete the EHE Contract Form that is used by EHE to determine appropriate funding source (OSP or UNIV).</p> <p>Respond to any inquiries from the FO, Chair, Associate Dean for Research, SFO or Legal Affairs as needed.</p>
Fiscal Officer	<p>Send DocuSign packet to initiator to complete.</p> <p>Review the information provided and the contract checklist to ensure the packet has the information needed for it to proceed through the contract portal and to determine if OSP should be involved.</p> <p>Identify any conflict of interest, if applicable.</p> <p>Approve or deny request as appropriate.</p> <p>Track DocuSign packet and follow up with initiator, Department, Chair, Associate Dean for Research, SFO, or the EHE Office of Research Admin Coordinator until it has been completed.</p> <p>Communicate denials to initiator and Chair.</p> <p>Once executable contract is returned, send a request to Assistant Director OFBS to establish a new contract fund.</p>
Department Chair	<p>Review request to ensure it's aligned with the mission of the department.</p> <p>Approve or deny request as appropriate. Discuss any concerns with FO and initiator prior to approving. Communicate denials to initiator and FO.</p>
Senior Fiscal Officer	<p>Review the information provided and the contract checklist to ensure the packet has the information needed for it to proceed through the contract portal and to determine if OSP should be involved.</p> <p>Identify any conflict of interest, if applicable.</p> <p>Review request to ensure it is aligned with the EHE vision and mission.</p> <p>Approve or deny request as appropriate. Communicate denials to FO.</p>
Associate Dean for Research	<p>Review the contract for appropriateness and alignment with EHE's research vision and mission.</p> <p>Approve or deny request as appropriate. Communicate denials to FO.</p> <p>For non-research related items, the Dean has delegated review to the Associate Dean for Research for consistency and alignment with the EHE vision and mission.</p>
EHE Office of Research Admin Coordinator	<p>Enter into the contract portal within 2 days of receiving DocuSign. Enter Signature of Completion in DocuSign with date entered into contract portal.</p> <p>Connect legal affairs with necessary parties as appropriate to answer questions.</p> <p>Notify EHE stakeholders of final approved contract.</p>


College of Education and Human Ecology
Office of Research

153 Arps Hall, 1945 N. High St.

Columbus, OH 43210

614-247-2412

Process as Contract?

If you answer "yes" to any of the following questions, your contract may need to be processed by the university Office of Sponsored Programs (OSP) in accordance with university policies and procedures.

	Yes	No
1. Does this contract include any areas which require regulatory oversight? <input type="checkbox"/> Human subjects <input type="checkbox"/> Vertebrate animal testing <input type="checkbox"/> Export control <input type="checkbox"/> Radioactivity use		X
2. Is the contracting agency part of the federal government? Federal Government Agency Name: _____		X
3. Does this contract involve Federal flow through funding, A21 (defines allowable costs) or A133 (outlines audit requirements) reporting requirements, which includes time and effort reporting?		X
4. Does this contract have cost-sharing requirements?		X
5. Will this contract produce publishable research or new knowledge with potential for commercialization?		X
6. Will this contract conduct a systematic investigation to develop, test, evaluate or contribute to generalizable knowledge?		X

Did you answer "yes" to any of the questions above? Please provide additional information below regarding the rationale.



College of Education and Human Ecology

Office of Research

153 Arps Hall, 1945 N. High St.

Columbus, OH 43210

614-247-2412

Contract Cover Sheet

LAC#: _____

Contracting Agency: Steven Point Area Public School District	
Primary EHE Contact: Jonathan Bailey	
Contract Amount (Indicate any overhead percentage.)	\$ 0 % 0
<p>Please check which fund is applicable and provide fund number if it exists: Agency Fund - Funds belong to an external entity; university acts as custodian of funds. The fund can't carry a deficit.</p> <p><input type="checkbox"/> Conference Fund - Provide a cash flow statement with details of associated fees.</p> <p><input type="checkbox"/> Earnings Fund - University entities that render goods or services to internal units or external customers. Provide approved fee schedule that supports contract fees.</p> <p><input type="checkbox"/> Contract Fund - Non-OSP fund for private/state contracts. Check here if contract involves the Office of Extended Education (EEEd).</p>	<p>Org: N/A</p> <p><i>Fill out fields below for conference & earnings funds only:</i></p> <p>Fund: N/A</p> <p>Project: N/A</p> <p>Program: N/A</p>
<p>REQUIRED: Contract Start Date: 12/16/2021 End Date: 06/30/2024</p>	
<p>Business Purpose: (Provide brief description of business purpose.) Define standards for use of data for analysis and evaluation services provided by IDEC to the Steven Point Area Public School District. No financial terms present. Data Privacy Agreement.</p>	
<p>Verifies approval of budget, overhead rate if any, supporting documents and fiscal review. Final contract will be returned to unit fiscal officer unless otherwise noted.</p>	<p>Signature: Unit Fiscal Officer DocuSigned by: Stephen A Pruchnicki X _____ FF750309DDB4435...</p>
<p>Verifies review and approval of contract.</p>	<p>Signature: Dept. Chair/Center Dir. DocuSigned by: Antoinette Cecilia Miranda X _____ C6EA7DF3FC524B2...</p>
<p>Verifies and approves that the fund and the fiscal criteria are satisfied. Recommendations by Director of Finance & Business Services: Requires Dean review and approval.</p>	<p>Signature: Director of Finance & Business Services DocuSigned by: Kelly Robinson Crawford X _____ E9C8BB4AD84D479...</p>
<p>Recommendations by Associate Dean to Dean: Requires Dean review and approval.</p>	<p>Signature: Associate Dean for Research DocuSigned by: Natasha Slesnick X _____ 19DDF3B0F0234DE...</p>

Charles Darren Parsons

12/17/2021

C:\ProgramData\activePDF\DC_ENT\Tmp\43ef84\b8495772-b5b4-4ff1-88a2-d1bb195688fd.c... 443481DF98BD4BA...

DocuSigned by:
 Charles Darren Parsons

**EHE Fiscal Officers Only**

Please ensure that you have reviewed the Contract Checklist below prior to routing for approval.

Note: If any item below is not checked, please explain why in space provided below.

<input checked="" type="checkbox"/>	The business terms negotiated by parties are contained in the contract or the term sheet.
<input checked="" type="checkbox"/>	The contract and all necessary exhibits are attached.
<input type="checkbox"/>	The payment terms are clearly stated and address the amount, timing and method of payment.
<input type="checkbox"/>	Any provisions that require the University to indemnify or hold harmless the other party have been removed.
<input type="checkbox"/>	Any confidentiality provisions have either been removed or are limited "to the extent permitted by Ohio law."
<input type="checkbox"/>	The contract clearly states that it is governed by the laws of the State of Ohio.
<input type="checkbox"/>	Does the contract require an exchange of Protected Health Information (PHI)?
<input type="checkbox"/>	Prior or existing contracts, if any, are attached.
<input checked="" type="checkbox"/>	I have reviewed this contract with the Dean, Vice President, Director or Chair of the Unit/Department/College requesting this review and that individual is aware of and approves all business terms of the contract.
<input checked="" type="checkbox"/>	The term of the contract is clearly stated and the contract addresses renewal (if applicable) and termination of the contract.
<input checked="" type="checkbox"/>	The signature blocks are clear and include the authorized signatories.
<input checked="" type="checkbox"/>	The contract does not include an indemnification obligation of the other party that requires such party to retain sole control of the defense and settlement of the University's claims.
<input checked="" type="checkbox"/>	The contract does not require the University to maintain a certain type or dollar amount of insurance.
<input checked="" type="checkbox"/>	There is no provision that requires the University submit to binding arbitration or mediation.
<input checked="" type="checkbox"/>	Is a bid waiver required? (If contract was not bid, a waiver is required for contracts \$25,000 or more for goods and \$50,000 or more for services).

Additional Information:

<p>No financial terms in contract.</p> <p>Language approved by OLA attorney Daniel Beerck.</p> <p>Contract governs use of student data required for IDEC to perform services, but I do not believe any data sets would qualify as PHI.</p>
--

WISCONSIN STUDENT DATA PRIVACY AGREEMENT

School District/Local Education Agency:

STEVEN POINT AREA PUBLIC SCHOOL DISTRICT

AND

Provider:

THE OHIO STATE UNIVERSITY

Date: December 16, 2021

This Wisconsin Student Data Privacy Agreement (“DPA”) is entered into by and between the [Steven Point Area Public School District] (hereinafter referred to as “LEA”) and [The Ohio State University] (hereinafter referred to as “Provider”) on December 16, 2021. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a contract dated December 16, 2021 (“Service Agreement”); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to Wisconsin state student privacy laws, including pupil records law under Wis. Stat. § 118.125 and notice requirements for the unauthorized acquisition of personal information under Wis. Stat. § 134.98; and

WHEREAS, for the purposes of this DPA, the Provider is a school district official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other LEAs in Wisconsin the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to the Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and applicable Wisconsin law, all as may be amended from time to time. In performing these services, the Provider shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, the Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:

[Collect data on students receiving the Reading Recovery literacy intervention and provide annual reports that can used to evaluate the effectiveness of the intervention.]

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”.

[Insert Categories of Student Data to be provided to the Provider]

4. **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 term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student 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 LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School District Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. The Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. The Provider shall respond in a timely manner (and no later than 30 days from the date of the request) to the LEA’s request for Student Data in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, the Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact the Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. The Provider shall notify the LEA as soon as possible in advance of a compelled disclosure to a Third Party.

5. **Subprocessors.** The Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA, as well as state and federal law.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Annual Notification of Rights.** The LEA shall include a specification of criteria under FERPA for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification.** LEA shall notify the Provider promptly of any known or suspected unauthorized access. LEA will assist the Provider in any efforts by the Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF THE PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. The Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation.** The Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure.** The Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, the Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any student data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes the Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. The Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement the Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, the Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall the Provider dispose of data pursuant to this provision unless and until the Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** The Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. The Provider is also prohibited from mining data for any purpose other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited. This section does not prohibit the Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of the Provider are set forth below. The Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** The Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. The Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** The Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes the Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. The Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, the Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, the Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. The Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

- f. Security Coordinator.** If different from the designated representative identified in Article VII, section 5, the Provider shall provide the name and contact information of the Provider’s Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. Subprocessors Bound.** The Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. The Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article. The Provider shall provide a list of all Subprocessors or subcontractors used by the Provider when requested by the LEA.
- h. Periodic Risk Assessment.** The Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, the Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. The Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

 - i.** The name and contact information of the reporting LEA subject to this section.
 - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv.** Whether the notification was delayed because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. The Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. The Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. The Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests the Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to the Provider, the Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, the Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, the Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

The Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA from the date of execution through 6/30/2024.

2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Brian Casey
Title: Director of Technology
Contact Information:
bcasey@pointschools.net
715-345-7393

The designated representative for the Provider for this Agreement is:

Name: Jonathan Bailey
Title: Business Manager
Contact Information:
helpdesk@idecweb.us
1100 Kinnear Rd, Rm 100
Columbus, OH 43212

The designated representative of the Provider's Security Coordinator for this Agreement is:

Name: Dwain Chandler
Title: Systems Manager
Contact Information:
helpdesk@idecweb.us
1100 Kinnear Rd, Rm 100

_Columbus, OH 43212_____

- b. Notification of Acceptance of General Offer of Privacy Terms.** Upon execution of Exhibit “E”, General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for notice of acceptance of the General Offer of Privacy Terms is:

Name: Jonathan Bailey_____

Title: Business Manager_____

Contact Information:
helpdesk@idecweb.us_____

1100 Kinnear Rd, Rm 100_____

Columbus, OH 43212_____

- 8. Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
- 9. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 10. Governing Law; Venue and Jurisdiction.** DELETED. [Space held for consistency in numbering].
- 11. Authority.** The Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion

thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. The Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

12. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

13. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to the 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 WITNESS WHEREOF, the parties have executed this Wisconsin Student Data Privacy Agreement as of the last day noted below.

Provider:

BY:  Date: 12/21/2021

Kristine Devine
Vice President of Operations and
Deputy CFO of Business & Finance

Printed Name: _____ Title/Position: _____

Local Education Agency:

BY:  Date: 12/21/2021

Printed Name: Brian Casey Title/Position: Director of Technology

EXHIBIT "A"

DESCRIPTION OF SERVICES

[The International Data Center (IDEC) is department of the College of Education and Human Ecology at The Ohio State University (OSU). 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. The documents that do contain personally identifiable information are only accessible to the Reading Recovery Teacher Leader.]

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	✓
	Other application technology metadata - 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	
	Student class attendance data	✓
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	✓
	Place of Birth	
	Gender	✓
	Ethnicity or race	✓
	Language information (native, preferred or primary language spoken by student)	✓
	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	
	Student disability information	✓
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information - Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
	Local (School district) ID number	

Student Identifiers	State ID number	
	Vendor/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.	
	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	Please list each additional data element used, stored or collected by your application	

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: The term “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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of the Provider’s software, website, service, or app, including mobile apps, whether gathered by the Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

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

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means all of the following: (1) Any information that directly relates to a pupil that is maintained by LEA;(2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee; and any information that meets the definition of a “pupil record” under Wis. Stat. § 118.125(1)(d). For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School District Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B) and Wis. Stat. § 118.125(2)(d), a School District 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 education records; and (3) Is subject to 34 CFR 99.33(a) and Wis. Stat. § 118.125(2) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by the Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Wisconsin and federal laws and regulations. Student Data as specified in Exhibit “B” is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of the Provider’s services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: “Student Personal Information” means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or the Provider, who the Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 pupil records. However, for the purpose of this Agreement, 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

[Name or District or LEA] directs [Name of Provider] to dispose of data obtained by the Provider pursuant to the terms of the Service Agreement between LEA and the Provider. The terms of the Disposition are set forth below:

<p><u>Extent of Disposition</u></p> <p>Disposition shall be:</p>	<p>_____ Partial. The categories of data to be disposed of are as follows:</p> <p>_____ Complete. Disposition extends to all categories of data.</p>
<p><u>Nature of Disposition</u></p> <p>Disposition shall be by:</p>	<p>_____ Destruction or deletion of data.</p> <p>_____ Transfer of data. The date shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, the Provider shall destroy or delete all applicable data.</p>
<p><u>Timing of Disposition</u></p> <p>Data shall be disposed of by the following date:</p>	<p>_____ As soon as commercially practicable</p> <p>_____ By (Insert Date) _____</p> <p>[Insert or attach special instructions]</p>

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of the Provider

Date

EXHIBIT “F”

DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENT]

Certificate Of Completion

Envelope Id: F8189BF945904B4C86DF1B962134A17B
Subject: EHE Contract Review Process
Source Envelope:
Document Pages: 25
Certificate Pages: 2
AutoNav: Enabled
Enveloped Stamping: Enabled
Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Status: Completed

Envelope Originator:
Stephen Anthony Pruchnicki
1050 Carmack Rd
Columbus, OH 43210
pruchnicki.3@osu.edu
IP Address: 67.149.185.218

Record Tracking

Status: Original
12/17/2021 8:31:01 AM

Holder: Stephen Anthony Pruchnicki
pruchnicki.3@osu.edu

Location: DocuSign

Signer Events

Stephen A Pruchnicki
Pruchnicki.3@osu.edu
Interim Finance Officer
Security Level: Email, Account Authentication (None)

Signature
Completed

Using IP Address: 67.149.185.218

Timestamp
Sent: 12/17/2021 8:38:40 AM
Viewed: 12/17/2021 8:38:56 AM
Signed: 12/17/2021 8:40:21 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Stephen A Pruchnicki
Pruchnicki.3@osu.edu
Interim Finance Officer
Security Level: Email, Account Authentication (None)

DocuSigned by:
Stephen A Pruchnicki
FF750309DDB4435...

Signature Adoption: Pre-selected Style
Using IP Address: 67.149.185.218

Sent: 12/17/2021 8:40:23 AM
Viewed: 12/17/2021 8:40:41 AM
Signed: 12/17/2021 8:43:07 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Charles Darren Parsons
parsons.389@osu.edu
Interim CIO
The Ohio State University
Security Level: Email, Account Authentication (None)

DocuSigned by:
Charles Darren Parsons
443481DF98BD4BA...

Signature Adoption: Pre-selected Style
Using IP Address: 128.146.152.101

Sent: 12/17/2021 8:43:09 AM
Viewed: 12/17/2021 8:54:11 AM
Signed: 12/17/2021 8:54:30 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Antoinette Cecilia Miranda
miranda.2@osu.edu
Interim Chair, Dept of Teaching and Learning
The Ohio State University
Security Level: Email, Account Authentication (None)

DocuSigned by:
Antoinette Cecilia Miranda
C6EA7DF3FC524B2...

Signature Adoption: Pre-selected Style
Using IP Address: 76.252.144.170

Sent: 12/17/2021 8:54:33 AM
Viewed: 12/17/2021 8:55:43 AM
Signed: 12/17/2021 8:55:52 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Signer Events

Kelly Robinson Crawford
 robinsoncrawford.1@osu.edu
 Director & SFO
 The Ohio State University
 Security Level: Email, Account Authentication
 (None)

Signature

DocuSigned by:


 E9C8BB4AD84D479...
 Signature Adoption: Pre-selected Style
 Using IP Address: 74.137.155.186

Timestamp

Sent: 12/17/2021 8:55:54 AM
 Viewed: 12/17/2021 9:17:16 AM
 Signed: 12/17/2021 9:17:36 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Natasha Slesnick
 slesnick.5@osu.edu
 Professor and Associate Dean for Research
 The Ohio State University
 Security Level: Email, Account Authentication
 (None)

DocuSigned by:

 19DDF3B0F0234DE...
 Signature Adoption: Pre-selected Style
 Using IP Address: 108.80.148.180

Sent: 12/17/2021 9:17:38 AM
 Viewed: 12/18/2021 8:39:13 AM
 Signed: 12/18/2021 8:39:23 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

In Person Signer Events**Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp****Witness Events****Signature****Timestamp****Notary Events****Signature****Timestamp****Envelope Summary Events****Status****Timestamps**

Envelope Sent	Hashed/Encrypted	12/17/2021 8:38:40 AM
Certified Delivered	Security Checked	12/18/2021 8:39:13 AM
Signing Complete	Security Checked	12/18/2021 8:39:23 AM
Completed	Security Checked	12/18/2021 8:39:23 AM

Payment Events**Status****Timestamps**

Certificate Of Completion

Envelope Id: 3780232C3D8E4689A1ED2875D8C88042	Status: Completed
Subject: Please DocuSign: IDEC - Steven Point FY22-24 Data Privacy Agreement LAC_220433.pdf	
Source Envelope:	
Document Pages: 29	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Gloria A Wood
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	1050 Carmack Rd
	Columbus, OH 43210
	wood.854@osu.edu
	IP Address: 173.88.126.152

Record Tracking

Status: Original	Holder: Gloria A Wood	Location: DocuSign
12/20/2021 7:34:03 PM	wood.854@osu.edu	

Signer Events

Kristine G. Devine
 Devine.99@osu.edu
 VP of Financial Operations
 The Ohio State University
 Security Level: Email, Account Authentication
 (None)

Signature

DocuSigned by:

 B684EBE1B133490...
 Signature Adoption: Pre-selected Style
 Using IP Address: 74.140.6.199

Timestamp

Sent: 12/20/2021 7:34:52 PM
 Viewed: 12/21/2021 9:51:27 AM
 Signed: 12/21/2021 9:53:04 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

In Person Signer Events**Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp****Witness Events****Signature****Timestamp****Notary Events****Signature****Timestamp****Envelope Summary Events****Status****Timestamps**

Envelope Sent	Hashed/Encrypted	12/20/2021 7:34:52 PM
Certified Delivered	Security Checked	12/21/2021 9:51:27 AM
Signing Complete	Security Checked	12/21/2021 9:53:04 AM
Completed	Security Checked	12/21/2021 9:53:04 AM

Payment Events**Status****Timestamps**

Certificate Of Completion

Envelope Id: E9CC4E184B5E463BA6EDA1D5772DF5B5	Status: Completed
Subject: Please DocuSign: IDEC - Steven Point FY22-24 Data Privacy Agreement LAC_220433 - V1.pdf	
Source Envelope:	
Document Pages: 30	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Gloria A Wood
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	1050 Carmack Rd
	Columbus, OH 43210
	wood.854@osu.edu
	IP Address: 173.88.126.152

Record Tracking

Status: Original	Holder: Gloria A Wood	Location: DocuSign
12/21/2021 11:31:58 AM	wood.854@osu.edu	

Signer Events

Kristine G. Devine
 Devine.99@osu.edu
 VP of Financial Operations
 The Ohio State University
 Security Level: Email, Account Authentication (None)

Signature

DocuSigned by:

 B684EBE1B133490...
 Signature Adoption: Pre-selected Style
 Using IP Address: 74.140.6.199

Timestamp

Sent: 12/21/2021 11:38:43 AM
 Viewed: 12/21/2021 11:47:09 AM
 Signed: 12/21/2021 11:48:46 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	12/21/2021 11:38:43 AM
Certified Delivered	Security Checked	12/21/2021 11:47:09 AM
Signing Complete	Security Checked	12/21/2021 11:48:46 AM
Completed	Security Checked	12/21/2021 11:48:46 AM
Payment Events	Status	Timestamps