

PRATTSBURGH CENTRAL SCHOOL DISTRICT DATA PRIVACY AGREEMENT

PRATTSBURGH CENTRAL SCHOOL DISTRICT

and

Curriculum Associates, LLC

This Data Privacy Agreement ("DPA") is by and between the Prattsburgh Central School District ("EA"), an Educational Agency, and Curriculum Associates, LLC ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information (as hereinafter defined) in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. De-identified Data:** means that data from which all personally identifiable information has been removed or obscured so that it does not identify individual and there is no reasonable basis to believe that the information can be re-identified or otherwise used to identify individual.
- 4. Disclose:** To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.
- 5. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 6. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 7. Eligible Student:** A student who is eighteen years of age or older.
- 8. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to

transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 9. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 10. Parent:** A parent, legal guardian or person in parental relation to the Student (as hereinafter defined).
- 11. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below. PII shall not include De-identified Data
- 12. Release:** Shall have the same meaning as Disclose.
- 13. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 14. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 15. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 16. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement. Subcontractors do not include Contractor's cloud hosting provider, and other vendors used in the ordinary course of business who perform technology and software development and maintenance services under Contractor's supervision on Contractor's internal systems.
- 17. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to Quote ID 268984.2 attached hereto and incorporated herein dated January 19, 2022 ("Service Agreement");

Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law. Contractor may use De-Identified Data for product development, product functionality and research purposes as allowed under FERPA.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies articulated herein.

5. Right of Review and Audit.

Upon written request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor undergoes regular security audits, and an executive summary report of such audit will be provided to the EA upon written request.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and Subcontractors who need to know the PII in order to provide the services and the disclosure of PII shall be limited to the extent necessary to provide such services. Contractor shall ensure that all such employees and Subcontractors with access to PII comply with the terms of this DPA.
- (b) Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor who will have access to PII. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such Subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such Subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and Subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its Subcontractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA and receipt of written request to return or destroy such PII from the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law., with the exception of backups, which are automatically deleted over time in accordance with Contractor's data retention and destruction policies. As applicable, upon expiration or termination of the Service Agreement, and upon receipt of a written request, Contractor shall transfer PII, in a format agreed to by the Parties to the EA, with the exception of backups as noted above.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, with the exception as noted above. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors, upon receipt of written request from the EA.
- (d) To the extent that Contractor and/or its Subcontractors continue to be in possession of any De-identified Data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify De-identified Data.
- (e) Curriculum Associates maintains the perpetual right to use De-Identified Data for product development, product functionality and research purposes, as permitted under FERPA.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: Prattsburgh Central School District
Title: Data Privacy Officer, Kory Bay
Address: 1 Academy Street
City, State, Zip: Prattsburgh, NY 14873
Email: bayk@prattsburghcsd.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its’ authorized users, as related to such investigations, will

be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
BY: [Signature] <i>Kristina McCracken</i>	BY: <i>Robert Waldron</i>
[Printed Name]	Robert Waldron
[Title]	Chief Executive Officer
Date:	Date: August 10, 2022

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints may be submitted to the DPO, Kory Bay via mail: Prattsburgh CSD, Data Privacy Officer, 1 Academy Street, Prattsburgh, NY 14873, by emailing dpo@prattsburghcsd.org , or by calling 607-522-6211. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.


CONTRACTOR	
[Signature]	
[Printed Name]	Robert Waldron
[Title]	Chief Executive Officer
Date:	August 10, 2022

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Curriculum Associates, LLC
Description of the purpose(s) for which Contractor will receive/access PII	See Quote 268984.1 – To allow access and use of Contractor’s educational software.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>January 1, 2022</u> Contract End Date <u>January 1, 2027</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, and upon receipt of written request, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data with the exception of backups as noted above.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>(i) Systems and servers are hosted in a cloud environment; (ii) our hosting provider implements network-level security measures in accordance with industry standards; (iii) we manage our own controls of the network environment; (iv) access to production servers is limited; (v) servers are configured to conduct daily updates; (vi) servers have anti-virus protection, intrusion protection, configuration control, monitoring/alerting, and automated backups; we conduct regular vulnerability testing.</p> <p>See Curriculum Associates' New York Student Data Privacy and Security Plan for additional information, attached hereto</p>
Encryption	Data will be encrypted while in motion and at rest. Yes


CONTRACTOR	
[Signature]	
[Printed Name]	Robert Waldron
[Title]	Chief Executive Officer
Date:	August 10, 2022

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	As a response is lengthy, see attached New York Student Data Privacy and Security Plan
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	As a response is lengthy, see attached New York Student Data Privacy and Security Plan
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Employees receiving training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Curriculum Associates does not provide any personally identifiable information to subcontractors. Employees are bound by confidentiality agreements signed at the time of hire.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Curriculum Associates follows documented "Security Incident Management Procedures".
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon written request of EA, we will remove all PII and educator data from our production servers
7	Describe your secure destruction practices and how certification will be provided to the EA.	Certification of destruction will be provided to EA upon receipt of written request of EA

8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See New York Student Data Privacy and Security Plan
---	---	---

Curriculum Associates®

Prepared For:

Penny Kephart
Prattsburgh Central Sch Dist
1 Academy St,
Prattsburgh, NY 14873

1/19/2022

Dear Penny Kephart,

Thank you for requesting a price quote from Curriculum Associates. The chart below provides a summary of the products and i-Ready Partner Services included. If you have any questions or would like any changes, please contact us.

Quote ID: 268984.1 Valid through: 12/31/2022

Product	List Price	Net Price
i-Ready	\$38,400.00	\$38,400.00
Professional Development	\$5,250.00	\$5,250.00
i-Ready Partners Services	\$7,500.00	\$0.00
<i>i-Ready Partners Services Includes:</i>		
<ul style="list-style-type: none"><i>Initial Implementation Services: Provisioning, Initial Rostering, Hosting, Technology Assessment</i><i>Account Management: Account Manager You Know On A First Name Basis, Implementation Guidance, Realtime Achievement Data After Every Assessment, Ongoing Data Management</i><i>Staff Development Consultation and Resources: Consultative services to help you plan and make the most of Professional Development sessions; Access to Online Educator Learning (OEL) Digital Courses, and i-Ready Central Self-Service Resources</i><i>Technical Support: Proactive Network Monitoring & Issue Notification, Annual Health Check, Technical Support</i>		
	List Total:	\$51,150.00
	Savings:	\$7,500.00
	Shipping/Tax/Other:	\$0.00
	Total:	\$43,650.00

Thank you again for your interest in Curriculum Associates.

Sincerely

Alicia Kraack

akraack@cainc.com

Please submit this quote with your purchase order

Curriculum Associates®

Quote ID: 268984.1 Date: 1/19/2022 Valid through: 12/31/2022

Prepared For:
 Penny Kephart
 Prattsburgh Central Sch Dist
 1 Academy St,
 Prattsburgh, NY 14873
 pkephart@prattsburghcsd.org
 (607) 522-3795

Your Representative:
 Alicia Kraack

 akraack@cainc.com

Prattsburgh Central Sch Dist 1 Academy St, Prattsburgh, NY 14873

Total Building Enrollment: 252, Grade Range: PK - 12

Product Name	Grade	Item #	Qty	List Price	Net Price	Total
Professional Development i-Ready Assessment and Personalized Instruction New User Package - Getting Good Data, Using Data to Plan Instruction, and Tailored Support	Multiple	19979.0	1	\$5,250.00	\$5,250.00	\$5,250.00
Subtotal:						\$5,250.00
Shipping:						\$0.00
Tax:						\$0.00
School Subtotal:						\$5,250.00

Prattsburgh Central School 1 Academy St, Prattsburgh, NY 14873

Total Building Enrollment: 252, Grade Range: PK - 12

Product Name	Grade	Item #	Qty	List Price	Net Price	Total
i-Ready Assessment and Personalized Instruction Math Site License 201-350 Students 5 Years	Multiple	14966.0	1	\$38,400.00	\$38,400.00	\$38,400.00
i-Ready Partners Implementation Support- Provisioning, Tech Support, Hosting, Data Management, Implementation Planning, Data Reviews, and Check ins (5 Years)	Multiple	27943.0	1	\$7,500.00	\$0.00	\$0.00
Subtotal:						\$38,400.00
Shipping:						\$0.00
Tax:						\$0.00
School Subtotal:						\$38,400.00

Total

List Total:	\$51,150.00
Savings:	\$7,500.00
Merchandise Total:	\$43,650.00
Voucher/Credit:	\$0.00
Estimated Tax:	\$0.00
Estimated Shipping:	\$0.00
Total:	\$43,650.00

Special Notes

F.O.B.: N. Billerica, MA 01862
Shipping: Shipping based on MDSE total
Terms: Net 30 days, pending credit approval
Fed. ID: #26-3954988

Please submit this quote with your purchase order

Y2

Curriculum Associates®

Information on Professional Development Sessions and COVID-19

Protecting the health and safety of the educators we serve and their students, as well as the health and safety of our employees, is of paramount importance to Curriculum Associates. While it is our preference to deliver PD sessions in person, circumstances related to COVID-19 may require us to provide sessions virtually instead. Curriculum Associates' policy is to only provide PD sessions in person where one of our employees can reach the session site by car and where adequate safety measures are in place to protect the health of our session leaders and participants. Curriculum Associates reserves the right to switch any session from in-person to virtual if we cannot reach a session site by car, if adequate safety measures cannot be put in place, or if Curriculum Associates determines that it would otherwise put its employees at risk to provide an in-person session.

If your school or district will not permit visitors at the time of a scheduled session, Curriculum Associates would be happy to provide an equivalent live, virtual session via videoconference. Similarly, Curriculum Associates will comply with your school or district's health and safety requirements regarding on-site visitors if we are given adequate advance notice. Our PD Operations team will work with school or district personnel to hold sessions in a manner that protects the safety of educators and your school community as well as Curriculum Associates employees.

We are pleased to be able to serve you in these challenging times and look forward to providing productive learning sessions to your staff. Any questions regarding scheduling in-person or virtual training sessions should be directed to pdoperations@cainc.com.

Unparalleled Service and Educator Support

The *i-Ready Partners* team was born from our core value: the quality of our services is as important as the quality of our products. Know that when you implement our programs, your local *i-Ready Partners* will be there to support your team every step of the way.

Service Components

Our *i-Ready Partners* team is tasked with helping you implement our programs to meet ambitious district goals. *i-Ready Partners* support includes:

- **An Account Manager You Know on a First-Name Basis:** Dedicated account managers are your point of connection to a powerful network of *i-Ready* experts focused on making your implementation successful.
- **Consultative Professional Development Planning:** Tailored professional development plans ensure that PD is tied to your implementation goals and that educators are equipped to optimize the use of our programs from day one.
- **Real-Time Achievement Data after Every Assessment:** Detailed student achievement analytics to empower data-driven practices in classrooms.
- **Educational Consultants to Help You Know What's Coming Next:** Educational consultants to keep you up to speed on our latest research, development, and best practices.
- **Technical Support and Health Checks:** Proactive support that anticipates and heads off issues before they start—and is there for you should they arise.



**Account
Management**



**Professional
Development**



**Educational
Consultants**



**Achievement
Analytics**



**Technical
Support**

Your *i-Ready* *Partners* Team

Dedicated to helping you implement *i-Ready* programs and achieve your district goals



Curriculum Associates®

Placing an Order

Email: orders@cainc.com | **Fax:** 1-800-366-1158

Mail:

ATTN: CUSTOMER SERVICE DEPT.

Curriculum Associates LLC

153 Rangeway Rd

North Billerica, MA 01862-2013

Please visit CurriculumAssociates.com for more information about placing orders or contact CA's customer service department (1-800-225-0248) and reference quote number for questions.

Please attach quote to all signed purchase orders. If tax exempt, please submit a valid exemption certificate with PO and quote in order to avoid processing delays. Exemption certificates can also be submitted to exempt@cainc.com.

Shipping Policy

Unless otherwise noted, shipping costs are calculated as follows:

Order Amount	Freight Amount	Order Amount	Freight Amount
\$74.99 or less	Max charge of \$12.75	\$5,000.00 to \$99,999.99	8% of order
\$75.00 to \$999.99	12% of order	\$100,000 and more	6% of order
\$1,000 to \$4,999.99	10% of order		

Please contact your local CA representative or customer service (1-800-225-0248) for expedited shipping rates. The weight limit for an expedited order is 500lbs.

Unless otherwise expressly indicated, the shipping terms for all deliveries is FOB CA's Shipping Point (whether to a CA or third party facility). Risk of loss and title is passed to purchaser upon transfer of the goods to carrier, standard shipping charges (listed above) are added to the invoice or included in the unit price unless otherwise specified.

Supply chain challenges outside of Curriculum Associates' control may impact inventory availability for print product. We recommend submission of purchase orders as soon as possible to help ensure timely delivery.

Payment Terms

Payment terms are as follows:

- With credit approval: Net 30 days
- Without credit approval: payment in full at time of order
- Accounts must be current before subsequent shipments are made

To ensure payment processing is timely and environmentally conscious, CA encourages ACH or wire payments. CA's bank remittance information is:

- Account Number: 4418064408 | Account Name: Curriculum Associates, LLC
- Bank Name: Wells Fargo Bank – San Francisco, CA
- ABA Routing: 121000248
- SWIFT Code (International Only): WFBUS6S
- Tax ID: 26-3954988

Please send any payment notifications to payments@cainc.com. Credit card payments are only accepted for purchases under \$50,000.

Invoice Receipt Preference

CA is pleased to offer electronic invoice delivery. Electronic invoice delivery allows CA to deliver your invoice in a timely and environmentally friendly manner. To request electronic invoice delivery please contact the CA Accounts Receivable team at invoices@cainc.com or by fax (1-800-366-1158). Please reference your quote number, provide a valid email address where the invoice should be directed, and indicate you would like to opt into electronic invoice delivery.

i-Ready®

Customer's use of i-Ready® shall be subject to the i-Ready Terms and Conditions of Use, which can be found at i-ready.com/support.

Return Policy

Except for materials sold on a non-refundable basis, purchaser may return, at purchaser risk and expense, purchased materials with pre-approval from CA's Customer Service within 12 months of purchase. Please examine your order upon receipt. Before returning material, call CA's Customer Service department (1-800-225-0248) for return authorization. When returning material, please include your return authorization number and the return form found on the CA website. i-Ready®, Toolbox®, and BRIGANCE® Online Management Systems may be returned for a pro-rated refund for the remaining time left on the contract. We do not accept returns on unused i-Ready or Toolbox licenses®, materials that have been used and/or are not in "saleable condition," and individual components of kits or sets including but not limited to BRIGANCE® Kits, Ready® student and teacher sets, and Ready Classroom® student and teacher sets. For more information about the return policy, please visit CurriculumAssociates.com/support/shipping-and-returns.



Student Data Privacy and Security Plan

Last Updated: January 1, 2021

Purpose.

Curriculum Associates ("CA") takes the protection of our customers' data and information, particularly student data, very seriously. The purpose of this New York Student Data Privacy and Security Plan is to inform our New York customers about our current data security policies and practices, which are intended to safeguard this sensitive information. CA handles customer data in a manner consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), New York Education Law §2-d, as well as other state student data privacy protection laws.

Scope.

This policy covers the collection, use, and storage of data that is obtained through the use of the products and related services accessible through the use of CA's proprietary *i-Ready*® platform, *i-Ready Connect*™. These include *i-Ready*® Assessment, *i-Ready Learning*, *i-Ready Learning Games*, *i-Ready Standards Mastery*, *i-Ready* reports and reporting tools, and the e-book versions and digital components of *Ready Classroom*™ Mathematics. All of these products and services are collectively referred to in this policy as "*i-Ready*." Note that there are separate terms applicable only to *Ready Teacher Toolbox*, an educator-only facing product. These separate terms are described at the end of this privacy statement.

Student Bill of Rights.

The Parents Bill of Rights for Data Privacy and Security ("Parents Bill of Rights") is attached as [Exhibit A](#).

Student Data Obtained and Collected.

CA receives certain information, which we receive pursuant to the school official exception under FERPA, from its school district customers to enable students to use *i-Ready*. The following information is generally provided to CA for each student user of *i-Ready*:

- student first and last name;
- date of birth;
- gender;
- ethnicity or race;
- student identification number;
- student school or class enrollment;
- student grade level;

- teacher name;
- English language learner status, and;
- eligibility for free- or reduced-price lunch.

Note that some of these data fields (such as ethnicity or race, ELL status, eligibility for free or reduced-price lunch) are not required for the use of *i-Ready*. However, where districts would like reporting capabilities based on these categories, they may choose to provide this information to CA.

Data We Do Not Collect.

CA never obtains or collects the following categories of information through the use of *i-Ready*:

- user biometric or health data;
- user geolocation data;
- student email addresses or social media profile information; or
- student mailing addresses or phone numbers, or other such “directory” information.

Usage Data.

When students use *i-Ready*, certain assessment results and usage metrics are also created. These results and usage metrics are used by CA as described below. While teachers and school administrators are able to access student information and related *i-Ready* usage data, this information is not made available to other students or the public.

How We Use Student Data.

CA only uses student data for education-related purposes and to improve teaching and learning, as described in more detail here. We receive this data under the “school official” exception under FERPA:

- **For Services.** CA only uses student-identifiable data provided by schools and/or school districts to make *i-Ready* available to that particular student, and to provide related reports and services to that student’s school and school district and its educators and administrators. CA uses student data collected from the use of *i-Ready* for the purpose of making *i-Ready* available to its customers and for improving its content and effectiveness.
- **For Reporting.** CA provides reporting capabilities to its educator customers, and these reports are generated based on *i-Ready* usage information.
- **For Account Support.** Customers’ usage data may also be used on an aggregated basis to allow CA’ account management, customer service and tech support teams to provide services that meet the specific needs of our educator customers.
- **Treatment as PII.** CA treats all student-identifiable data, and any combination of that data, as personally-identifiable information, and that data is stored securely as described more fully below.
- **No Solicitation of Students.** CA receives education records from our school district customers to enable students and teachers to use *i-Ready*. CA does not solicit personally identifiable information directly from students—all student information is provided by school district customers or created through the use of the *i-Ready* platform. Because *i-Ready* is only used in the context of school-directed learning, schools are not required to obtain parental consent under COPPA to provide us with this data, although many customers choose to do so to comply with state or local requirements.
- **No Ownership.** CA does not obtain any ownership interest in student-identifiable data.

How We Use De-Identified Data.

- CA collects and uses “de-identified student data”, which refers to data generated from usage of *i-Ready* from which all personally identifiable information has been removed or obscured so that it does not identify individual students and there is no reasonable basis to believe that the information can be used to identify individual students.
- CA uses this aggregated, de-identified student data for core product functionality to make *i-Ready* a more effective, adaptive product.
- CA uses de-identified data to provide services to our educator customers. We sometimes use third party software tools (such as Salesforce or Domo) to enhance the level of service we provide. However, we only use de-identified data with these tools.
- CA also uses de-identified student data for research and development purposes. This might include research analyzing the efficacy of *i-Ready* or development efforts related to our product and service offerings. We also conduct research using de-identified data for studies focused on improving educational systems and student outcomes more generally.
- While some of this research work is done internally, CA does share de-identified student data with trusted third-party research partners as part of these research initiatives.
- CA does not attempt to re-identify de-identified student data and takes reasonable measures to protect against the re-identification of its de-identified student data.
- Our research partners are prohibited from attempting to re-identify de-identified student data.
- CA does not sell student identifiable data or aggregated de-identified student data to third parties.

No Targeted Advertisements or Marketing.

- CA does not include advertisements or marketing messages within *i-Ready* nor does it use student data for targeted advertising or marketing.
- No student data collected in connection with *i-Ready* usage is shared with third parties for any advertising, marketing, or tracking purposes.

No User Interactions.

- There are no social interactions between users in *i-Ready*, and a given user’s account is not accessible to other student users or third parties. Thus there is no opportunity for cyberbullying within *i-Ready*.
- There is no ability for users to upload user content created outside of *i-Ready*. Other than responses to questions or instructional prompts, students cannot create content within *i-Ready*.
- *i-Ready* user information does not involve the creation of a profile, and cannot be shared for social purposes.

Student Privacy Pledge.

To further demonstrate its commitment to protecting the privacy of student information, CA has taken the Student Privacy Pledge <https://studentprivacypledge.org/>. This means that, among other things, CA has pledged not to sell student information, not to engage in behaviorally targeted advertising, and to use collected data for authorized purposes only. CA only uses collected student data for the purposes described in the “How We Use Student Data” paragraph.

How We Use Educator Data.

CA also collects the following information about educators that use the *i-Ready* platform: name, school or district affiliation, grade level teaching, and email address. CA uses this information for account registration and maintenance purposes. CA also records when educator account logins are created, and when educators log in and out of the *i-Ready* platform. CA utilizes a third-party service provider to host professional-development content for educators in a learning-management system (LMS). For any educator who utilizes that content, CA and/or the educator will provide certain *i-Ready* account information to its third-party service provider, and this information will be used to communicate with educators and district-level administrators more effectively about their specific implementation and to better understand how educators use the *i-Ready* and LMS platforms.

Data Storage Location.

- *i-Ready* is a cloud-based application.
- Our servers are located in Tier 1 data centers located in the United States.
- We do not store any student data outside of the US.

Network-Level Security Measures.

- CA's *i-Ready* systems and servers are hosted in a cloud environment.
- Our hosting provider implements network-level security measures in accordance with industry standards.
- Curriculum Associates manages its own controls of the network environment.

Server-Level Security Measures.

- Access to production servers is limited to a small, identified group of operations engineers who are trained specifically for those responsibilities.
- The servers are configured to conduct daily updates for any security patches that are released and applicable.
- The servers have anti-virus protection, intrusion detection, configuration control, monitoring/alerting, and automated backups.
- Curriculum Associates conducts regular vulnerability testing.

Computer/Laptop/Device Security Measures.

Curriculum Associates employs a full IT staff that manages and secures its corporate and employee IT systems. Laptops are encrypted and centrally managed with respect to configuration updates and anti-virus protection. Access to all CA computers and laptops is password-controlled. CA sets up teacher and administrator accounts for *i-Ready* so that they are also password-controlled. We support customers that use single sign on (SSO) technology for accessing *i-Ready*.

Encryption.

- *i-Ready* is only accessible via https and all public network traffic is encrypted with the latest encryption standards.
- Encryption of data at rest is implemented for all data stored in the *i-Ready* system.

Employee and Contractor Policies and Procedures.

CA limits access to student- identifiable data and customer data to those employees who need to have such access in order to allow CA to provide quality products and services to its customers. CA requires all employees who have access to CA servers and systems to sign confidentiality agreements. CA requires its employees and contractors who have access to student data to participate in annual training sessions on IT security policies and best practices. Any

employee who ceases working at CA is reminded of his or her confidentiality obligations at the time of departure, and network access is terminated at that time.

Third-Party Audits and Monitoring.

In addition to internal monitoring and vulnerability assessments, Curriculum Associates contracts with a third party to conduct annual security audits, which includes penetration testing of the *i-Ready* application. Curriculum Associates reviews the third-party audit findings and implements recommended security program changes and enhancements where practical and appropriate.

Data Retention and Destruction.

Student and teacher personal data is used only in the production systems and only for the explicitly identified functions of the *i-Ready* application. Student and teacher personal data is de-identified before any testing or research activities may be conducted. Upon the written request of a customer, Curriculum Associates will remove all personally identifiable student and educator data from its production systems when CA will no longer be providing access to *i-Ready* to that customer. In addition, CA reserves the right, in its sole discretion, to remove a particular customer's student data from its production servers a reasonable period of time after its relationship with the customer has ended, as demonstrated by the end of contract term or a significant period of inactivity in all customer accounts. Student data is removed from backups in accordance with CA's data retention practices. If CA is required to restore any materials from its backups, it will purge all student-identifiable data not currently in use in the production systems from the restored backups.

Correction and Removal of Student Data.

- Parents of students who use *i-Ready* may request correction or removal of their child's personally identifiable data from *i-Ready* by contacting their child's teacher or school administrator. The teacher or school administrator can then verify the identity of the requesting party and notify CA of the request.
- CA will promptly comply with valid requests for correction or removal of student data; however, removal of student personally identifiable data will limit that student's ability to use *i-Ready*.

Breach Notification.

CA follows documented "Security Incident Management Procedures" when investigating any potential security incident. In the event of a data security breach, CA will notify impacted customers as promptly as possible that a breach has occurred, and will inform them (to the extent known) what data has been compromised. CA expects customers to notify individual teachers and parents of any such breach to the extent required, but will provide customers reasonably requested assistance with such notifications and will also reimburse customers for the reasonable costs associated with legally required breach notices.

Data Collection and Handling Practices for All Teacher Toolboxes.

The Teacher Toolbox for *Ready Classroom Mathematics*, *Ready Mathematics*, *Ready Reading*, and *Ready Writing* provides a set of digital resources intended for use by educators. It is not a student-facing product, and therefore no student data is collected through the use of any Teacher Toolboxes. CA collects the following information about educators who use a Teacher Toolbox: name, school or district affiliation, grade level teaching, and email address. CA uses this information for account registration and maintenance purposes. CA also records when educator account logins are created, and when educators log in and out of Teacher Toolbox. When a teacher uses a Teacher Toolbox, our systems record which resources have been accessed by whom and the frequency of access. We use this information for product development purposes, to ensure that we are providing educators with resources that are useful to them. Our account management, customer service and tech support teams also use this information to provide more specifically tailored support to our educator customers. Upon request, we may also provide this information to school or district level administrators to

help them better understand how our Toolbox resources are used by educators in their school or district. We also use this information to communicate with educators more effectively about their specific implementation. We do not sell this information or otherwise share it with any third parties, nor do we serve advertisements to educators based on this usage data. We do not use this data to create a profile about any of the educators who use our products to provide to anyone outside of CA. We simply use this collected data for internal purposes to make our product and service offerings better.

If you have any questions about our data handling practices or this privacy policy, you may contact us at privacy@cainc.com.

This plan is being provided in accordance with Part 121.6 of the Regulations of the Commissioner of Education pursuant to NYS Ed Law 2-d

Exhibit A

Parents Bill of Rights for Data Privacy and Security

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by the school district is available from the school district.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints should be submitted directly to the school district.
7. To be notified by the school district in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Curriculum Associates, LLC

Dow Hardy

4A67A4FABA26427...
Name: Dow Hardy

Title: VP, Technology and Chief Information Security Officer