



31 Emory Ave
Cazenovia, NY 13421

JENNIFER RAUX
Director of Instructional Technology

Phone: 315.655.1314, X.5380

DATE: June 19, 2023

To Whom it May Concern:

RE: <Physics Classroom> Agreement with Cazenovia Central School District

The Cazenovia Central School District would like to contract with your company for the above referenced program/service. Attached you will find the agreement between your company and the Cazenovia Central School District concerning the NYS Ed Law and Regulations 121, Data Security and Privacy. Please review the agreement and return signed to Jennifer Raux, Director of Instructional Technology via email.

Please note the following areas of the document that require your attention:

- Page 1 Service vs. License
- Page 1 Term of service
- Page 4 Signature
- Page 5 Addendum A
- Page 6-8 Addendum B
- Page 9 Addendum C
- Page 11 Addendum E
- Page 12-13 Addendum F

Sincerely,

Jennifer Raux
Director of Instructional Technology, Data Protection Officer
Cazenovia Central School District
31 Emory Ave
Cazenovia, NY 13035
jraux@caz.cnyric.org

315-655-1314 ext. 5380

Software Vendor Agreement

Cazenovia Central School District



This Agreement, made and entered into <June 19, 2023> (Effective Date), by and between <Physics Classroom>, having offices at <Vendor Address> (“Vendor”), and the Cazenovia Central School District, having an office at 31 Emory Avenue, Cazenovia, New York 13035 (“School District”) (collectively “Parties”).

In consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. PICK ONE

- **Services.** Vendor shall perform the services set forth in this Agreement, as described in Addendum A (the “Services”). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.
- 2. Data Accessed by Vendor.** Vendor shall identify categories of all data accessed by Vendor or its subcontractors as part of this Agreement as set forth in Addendum B.
- 3. Term of Services.** This Agreement begins on 8/1/2023 and will continue unless terminated pursuant to Section 4 below (the “Term”).
- 4. Termination.** This Agreement may be terminated as follows:
 - (a) By the School District upon thirty (30) days prior written notice to Vendor;
 - (b) By the School District immediately in the event of breach by the Vendor; and
 - (c) By either Party upon written mutual agreement.
- 5. Payment.** Payment shall be made in accordance with Addendum C attached hereto.
- 6. Protection of Confidential Data.** Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR § 121.1(q)) and Teacher or Principal Data (as defined by 8 NYCRR § 121.1(r)) (hereinafter “Confidential Data”) in accordance with the requirements articulated under Federal, State and local laws and regulations, including but not limited to the foregoing:
 - (a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.
 - (b) Vendor will comply with the School District Data Security and Privacy Policy, Education Law § 2-d, and 8 NYCRR § 121.
 - (c) Vendor will limit internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services.

- (d) Vendor will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.
- (e) Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.
- (f) Vendor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.
- (g) Vendor will use encryption to protect personally identifiable information in its custody while in motion or at rest.
- (h) Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.
- (i) In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

7. Data Breach. In the event that Confidential Data is accessed or obtained by an unauthorized individual, Vendor shall provide notification to the School District without unreasonable delay and not more than seven (7) calendar days after the discovery of such breach. Vendor shall follow the following process:

- (a) The security breach notification shall be titled "Notice of Data Breach," shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery; a description of the types of Confidential Data affected; an estimate of the number of records affected; a brief description of the Vendors investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions.
- (b) The Vendor shall also prepare a statement for parents and eligible students which provides information under the following categories: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."
- (c) Where a breach or unauthorized release of Confidential Data is attributed to Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the cost of notification to parents and eligible students of the breach.

- (d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Data.
 - (e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and Federal and State laws for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Confidential Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District.
- 8. **Indemnification.** Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees, and students (collectively for purposes of this Section, “the School District”), from and against any and all settlements, losses, damages, costs, counsel fees and all other expenses relating to or arising from (a) Vendor’s failure to comply with the terms of this Agreement; and/or (b) the negligent operations, acts or omissions of the Vendor.
- 9. **Compliance with Laws.** Vendor, its employees and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.
- 10. **Independent Relationship.** It is expressly intended by the Parties hereto, and Vendor hereby specifically warrants, represents and agrees, that Vendor and the School District are independent entities. The Parties intend that this Agreement is strictly between two independent entities and does not create an employer/employee relationship for any purpose. Vendor shall perform the duties contemplated by this Agreement as an independent entity, to whom no benefits shall accrue except for those benefits expressly set forth in this Agreement.
- 11. **Assignment.** This Agreement is binding upon the Parties and their respective successors and assigns, but Vendor’s obligations under this Agreement are not assignable without the prior written consent of the School District. Any assignment without the School District’s consent shall be null and void.
- 12. **Governing Law.** This Agreement and any Services provided hereunder shall be governed by the laws of the State of New York both as to interpretation and performance, without regard to its choice of law requirements.
- 13. **Waiver.** No delay or omission of the School District to exercise any right hereunder shall be construed as a waiver of any such right and the School District

reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

- 14. Addendums.** The following Addenda are attached hereto and incorporated herein:
- Addendum A: Description of Specifications and Services
 - Addendum B: Schedule of Data
 - Addendum C: Payment Schedule
 - Addendum D: School District’s Parents’ Bill of Rights
 - Addendum E: Parents’ Bill of Rights – Supplemental Information Addendum
 - Addendum F: Vendor’s Data Security and Privacy Plan
- 15. Severability.** Should any part of this Agreement for any reason be declared by any court of competent jurisdiction to be invalid, such decision shall not affect the validity of any remaining portion, which remaining portion shall continue in full force and effect as if this Agreement had been executed with the invalid portion hereof eliminated, it being the intention of the Parties that they would have executed the remaining portion of this Agreement without including any such part, parts or portions which may for any reason be hereafter declared invalid.
- 16. Entire Agreement.** This Agreement and its Addendums constitute the entire Agreement between the Parties with respect to the subject matter hereof and shall supersede all previous negotiations, commitments and writings. It shall not be released, discharged, changed or modified except by an instrument in writing signed by a duly authorized representative of each of the Parties.

IN WITNESS WHEREOF, the Parties have signed this Agreement intending to be legally bound.

The Physics Classroom, LLC	Cazenovia Central School District
By: <i>Thomas J. Henderson</i>	By: Jennifer Raux
Name: Thomas J. Henderson	Name: <i>Jennifer Raux</i>
Title: Owner	Title: Director of Instructional Technology
Date: 6/19/2023	Date: 6/19/23

Addendum A: Description Of Specifications And Services

Description of Services

The Physics Classroom provides subscriptions that allow teachers to track the progress of their students on interactive website tasks.

Product Specifications

This is an online tool. To access the tool, students will need an account. Student accounts require the use of a username that is formatted in the form of an email address; we recommend the use of the school email address. At a minimum, a first name and last initial needs to be associated with the account; we recommend a first and last name.

As of this writing, we will track progress on the following website sections: Concept Builders, Minds On Physics, The Calculator Pad, Concept Checkers for Physics Interactives, and the Science Reasoning Center. Further details are available on our website.

Because we are a free website, we utilize targeted ads on the perimeter of the pages to offset our costs while providing a free website with low-cost premium services. We do not share or use or distribute in any way personally identifying data to support our ad program. We offer ad-free subscriptions at an additional cost for schools who would prefer to opt out of the ad displays; once logged in, a student on an ad-free subscription will not view ad displays.

Technical Specifications

Our product requires a modern browser that is HTML5-compliant.

Addendum B: Schedule of Data

Category of Data	Elements	Check if used by your system
Application of Technology Metadata	IP Addresses, Use of cookies, etc.	X
	Other application technology metadata (specify):	
Application Use Statistics	Metadata on user interaction with applications	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify):	
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 (specify):	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (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	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information (specify):	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School District) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	X

	Student app passwords	X
Student Name	First and/or Last	X
Student In-App Performance	Program/application performance (ex: typing program-student types 60 wpm, reading program-student reads below grade level)	X
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 transportation data (please specify):	
Other	Please list each additional data element used, stored or collected by your application	

Addendum C: Payment Schedule

We accept purchase orders. While it isn't going to break the deal, we hope schools/districts make payments within 60 days of registration.

The subscriptions can be purchased in our Store using either a credit card or by indicating that a purchase order will be used and payment will come at a later time.

Addendum D: Cazenovia Central School District Parents' Bill Of Rights

EDUCATION LAW §2-D 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) of the Cazenovia Central School District 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. 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 NYSED is available at <http://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. Complaints may be submitted to NYSED at <http://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.

Addendum E: Parents' Bill Of Rights – Supplemental Information Addendum

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which “student data” or “teacher or principal data” (as those terms are defined in Education Law Section 2-d and collectively referred to as the “Confidential Data”) will be used by <Physics Classroom> (the “Vendor”) are limited to the purposes authorized in the contract between the Vendor and Cazenovia Central School District (the “School District”) dated <June 19, 2023> (the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to, those outlined in applicable State and Federal laws and regulations (e.g., Family Educational Rights and Privacy Act (“FERPA”); Education Law § 2-d; 8 NYCRR § 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District in [CSV format] format and/or destroyed by the Vendor as directed by the School District.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any “education record”, as that term is defined in the FERPA, stored by the School District in a Vendor’s product and/or service by following the School District’s procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Vendor’s product and/or service by following the appeal procedure in the School District’s APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the School District will be stored [on servers at Heartland Business Systems in Little Chute, WI]. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum F: Vendor’s Data Security and Privacy Plan

WHEREAS, the Cazenovia Central School District (hereinafter “School District”) and The Physics Classroom, LLC (hereinafter “Contractor”) entered into an agreement dated 6/19/2023 (hereinafter “Agreement”) for a Task Tracker subscription (hereinafter “Services”).

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s):

Our website is hosted on the servers owned by Heartland Business Systems (HBS). The information assets of Heartland and its customers are an integral part of their daily operations, and the organization has made a substantial investment in the creation, upkeep, and usefulness of the information assets it possesses. Heartland also understands it has legislative, regulatory, and contractual obligations regarding the protection and confidentiality of information under its control. Without access to its information assets and the capability to process new information, the organization would quickly lose substantial revenue.

Given the dependency of the organization on information and information technology an information Security function and Program have been created. The primary goal of information Security is to protect the information assets of the organization from unauthorized or accidental modification, destruction or disclosure. Secondary goals of the Information Security Program are focused on the following tenants of information assurance:

Confidentiality: Ensure that only authorized individuals’ access or view information that has been deemed privileged.

Integrity: Ensure that information is unchanged from its source to destination or remains unchanged from unauthorized modifications while at rest.

Availability: Ensure that information is readily accessible and available for use.

The following guiding principles are used to form the structure of our program:

- The NIST Cyber Security Framework (CSF) is used as the base framework for the program.
- Necessary information security components needed to comply with relevant laws, regulations, and mandates are layered in. These include HIPAA, PCI, as well as applicable State and Federal Privacy Laws.

The Information Security Policies are fundamental components of the Information Security Program. These policies define the overall information Security expectations, responsibilities, and compliance requirements of the organization. The overall Information Security Policy lists the mandatory supporting policies, procedures, standards, and guidelines required by the organization. It also defines the ownership of the policy, and defines the timetables for policy review.

Company Management and the Information Security Steering Committee approves and supports all Information Security Policies, adherence is mandatory by all employees and contractors. Non-compliance or violations of Information Security policies could result in disciplinary actions ranging from reprimands to termination and/or legal action.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

See above answer.

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.
 - a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
 - b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.
 - c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.
 - d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.
 - e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided: Specify date of each training

I am the sole employee and I stay continuously informed with respect to all data privacy laws.

5. Subcontractors (check one):

- Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

Employees are required to complete Security awareness training upon hire and annually thereafter. Heartland requires its employees to sign written agreements requiring the employees to protect the confidentiality of customer information.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.

Data security and privacy incidents are handled according to the data center incident response plan. HBS will report breaches or unauthorized disclosures directly to the EA within 3 business days of a confirmed breach or unauthorized disclosure.

7. Termination of Agreement.

- a. On August 30, 2024 (or earlier if the teacher designates so in the Class settings), Contractor shall delete or destroy all student data or teacher or principal data in its possession.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 6/19/2023.

Contractor	The Physics Classroom, LLC
By	Thomas J. Henderson
Title	Owner

[Data Privacy and Security Privacy Policy - Cazenovia CSD](#)

EDUCATION LAW §2-D 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 NYSED is available at <http://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. Complaints may be submitted to NYSED at <http://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.

