CAZENOVIA
CENTRAL SCHOOL DISTRICT

A TRADITION OF
EXCELLENCE & EQUITY

31 Emory Ave
Cazenovia, NY 13421

JENNIFER RAUX
Director of Instructional Technology

Phone: 315.655.1314, X.5380

DATE: July 12, 2023

To Whom it May Concern:

RE: Lightspeed Solutions, LLC dba Lightspeed Systems 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 Jul 12, 2023 <**contract date**> (Effective Date), by and between Lightspeed Solutions, LLC dba Lightspeed Systems, having offices at 12013 Fitzhugh Road, Austin, TX 78736 ("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.]**OR**
   - ☒[**License**. Vendor hereby grants to School District, including to all School District's authorized users, a non-exclusive, non-sublicensable, non-assignable and royalty-free license to access and use the service (the "Services") solely for School District's operations in accordance with the terms of this Agreement.

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 the Effective Date 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.

Lightspeed Solutions, LLC dba Lightspeed Systems	**Cazenovia Central School District**
By:	By:
Name: Gregory Funk	Name: Jennifer Raux
Title: VP, Corporate Controller	Title: Director of Instructional Technology
Date: Jul 12, 2023	Date: July 17, 2023

Addendum A: Description Of Specifications And Services

Description of Services

Lightspeed Alert is an at-risk student identification solution that monitors and analyzes student online activity for signs of self-harm, violence, and bullying. By enabling early intervention,

Lightspeed Alert empowers schools to take a proactive approach to student safety.

- Comprehensive coverage provides visibility into early warning signs. Our SmartAgents and extended cloud integrations provide coverage across web browsers, social media, YouTube, and Microsoft 365 and Google productivity apps.
- Our patented AI technology identifies concerning online indicators and alerts designated staff. Alerts include relevant context with recent web searches and site history, enabling staff to quickly understand the situation and take action.
- An experienced human review team augments staff resources. Highly trained team members with backgrounds in law enforcement, mental health, and education work 24/7/365 to evaluate all alerts and escalate those that indicate a potential critical event.

Product Specifications

Lightspeed Alert™ combines smart AI technology that encompasses machine learning and context Lightspeed Alert™ delivers real-time alerts protecting students beyond content-filtering. When triggered an alert will immediately be sent to designated team members for review and action. Notifications include web history and screenshots in alert for instant review. The combination of these two technologies drastically decreases the number of false positives seen by numerous other products, preventing the designated team members from becoming overwhelmed by alerts.

Lightspeed Alert™ advance reporting allows designated team members to easily see the browsing traffic 5 minutes before any alert, and a screenshot of the alert. Ensuring that the staff member can make a quick and efficient decision regarding the incident. This system alerts across all internet traffic, not just GSuite for Education Products or O365 products, like other products are limited to.
Lightspeed Alert™ also provides 24/7/365 human review of all student safety alerts.

Here's how it works:
Our patented AI technology flags alerts of concerning student online behavior, including self-harm and violence indicators, and sends those alerts to district-designated staff.
Trained Lightspeed safety specialists review and analyze all alerts for context, threat level, and imminence. If imminent danger to the student or school exists, safety specialists will follow an escalation process, including contacting law enforcement to intervene.

Technical Specifications

- Comprehensive Protection: Get critical alerts across the internet—images, social media, online docs, email, YouTube, apps, browsers, search engines, and more—no matter where devices are used.
- Advanced AI: Leverage our advanced AI to get the information you need to keep students safe while also separating signal from noise.
- Lightspeed Safety Specialists: Each safety specialist is a full-time Lightspeed employee and receives comprehensive training in conjunction with threat assessment resources and suicide prevention groups.
- Ability to See Context: Lightspeed Alert works seamlessly with Lightspeed Filter to provide full context into what a student was doing before and after an alert occurred.
- Fast and Accurate Roster Syncing: Simultaneously sync any combination of Student Information Systems (SIS) and directory services to one centralized place with SmartSync™ technology.

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.	☒
	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	☒
	Phone	
Student Identifiers	Local (School District) ID number	☒
	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 (ex: 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 transportation data (please specify):	

Other	Please list each additional data element used, stored or collected by your application **List of other Student Information collected** **Lightspeed Alert (Human Review)™ - -** https://www.lightspeedsystems.com/products/lightspeed-alert/ • Alert search history, incident URL and screenshot of activity • Username • User Type (student or staff) • Websites that users at the school visited • Specific Search Queries of Users	☒

Addendum C: Payment Schedule

Payment agreements are between Cazenovia Central School District and CDW.

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 Lightspeed Solutions, LLC dba Lightspeed Systems (the "Vendor") are limited to the purposes authorized in the contract between the Vendor and Cazenovia Central School District (the "School District") dated Jul 12, 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 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 in secure data centers located in the United States. 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 Lightspeed Solutions, LLC dba Lightspeed Systems (hereinafter "Contractor") entered into an agreement dated Jul 12, 2023 (hereinafter "Agreement") for Lightspeed Alert™ Human Review (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):

Lightspeed Systems will comply as follows:

- Employ safeguards which align with the NIST Privacy & Security Frameworks.
- Limit internal access to personally identifiable information to only those employees or sub-contractors with a legitimate business need to provide the contracted services.
- Maintain adequate organizational, technical and physical safeguards, to protect the security, confidentiality and integrity of the School District personal information in our custody.
- Subcontractors will be contractually bound to observe the same obligations to maintain data privacy and security as required by the School District, and pursuant to this Agreement.
- Encrypt data in transit and at rest
- Please visit our Trust page for our detailed data security practices

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:

- Lightspeed Systems has implemented and maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody
- Our safeguards and practices align with the NIST Cybersecurity Framework
- We Use encryption to protect personally identifiable information in our custody while in motion or at rest
- We have implemented policies and procedures for data protection, such as but not limited to, Incident Response Plan, Security Policy, Data Deletion Policy, Vulnerability Remediation Policy, Vendor Assessment Policy and Password Policy.

- Data breach notification: If we learn of a data breach, we will follow our Incident Response Plan and notify our customers without undue delay.
- Employee training is in place before hire and ongoing on data protection practices
- Access controls are in place, and only employees with a legitimate business need have access to data
- All vendors are assessed before engagement, and on an ongoing basis, to ensure they have adequate data protection practices.
- Written Agreements are in place with all sub-processors, which bind them to strict data protection practices
- Lightspeed Systems has a Vulnerability Remediation policy to identify and remediate vulnerabilities according to the risk they present. We utilize patch management software to monitor systems and ensure patches are implemented.
- Please visit our Trust page for our detailed data security practices

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

- Lightspeed Systems trains all employees/contractors upon hire and on an annual basis on data privacy laws such as, but not limited to COPPA, FERPA, NY Ed Law 2d and GDPR. Data security training is also provided, as well as regular phishing exercises to ensure diligence and data protection.
- Training on safe handling of data is also administered.

5. Subcontractors (check one):

- Contractor shall not utilize subcontractors.
- ☒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:

• Lightspeed Systems may use sub-contractors to perform services and are only entitled to access customer data only as needed to perform the Services and shall be bound by written agreements that require them to provide strict levels of data protection required by Lightspeed and applicable regulations. • Pre-engagement and ongoing vendor assessments are conducted to ensure proper data privacy and security practices are in place throughout the vendor relationship. • Changes to vendor services provided or changes to existing contracts require a security risk assessment to confirm that the changes do not present additional or undue risk.

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.

• Lightspeed Systems has a formal Incident Response Plan which details the processes for detecting, reporting, identifying, analyzing, and responding to Security Incidents impacting our networks and Customer Data. • Additionally, we have in place a Vulnerability Remediation policy to identify and remediate vulnerabilities according to the risk they present. • We utilize patch management software to monitor systems and ensure patches are implemented. • We also have anti-malware and anti-spam solutions to protect servers and workstations. If Lightspeed Systems learns of a data breach, we will follow our Incident Response Plan and notify the School District without undue delay.

7. Termination of Agreement.

a. Within **30 calendar** days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. Within **30 calendar** days of termination of the Agreement, Contractor shall
   - Return all data to the School District using _____; OR
   - Transition all data to a successor contractor designated by the School District in writing using _____.
   - ☒Securely transfer data to the School District, or a successor contractor at School District's option and written discretion, in a format agreed to by the parties.

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 Jul 12, 2023 **<contract date>**.

Contractor	Lightspeed Solutions, LLC dba Lightspeed Systems
By	Gregory Funk
Title	VP, Corporate Controller

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.

V1_06052020

Cazenovia Central School District_Lightspeed Systems_EdLaw 2d Agreement_20230712

Final Audit Report 2023-07-12

Created:	2023-07-12 (Central Daylight Time)
By:	Fiona Wright (fwright@lightspeedsystems.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAD62QAI3RL2PfC1HNqErWQz-PFkqlVn4s

"Cazenovia Central School District_Lightspeed Systems_EdLaw 2d Agreement_20230712" History

Document created by Fiona Wright (fwright@lightspeedsystems.com)
2023-07-12 - 3:22:12 PM CDT

Document emailed to Gregory Funk (gfunk@lightspeedsystems.com) for signature
2023-07-12 - 3:27:25 PM CDT

Email viewed by Gregory Funk (gfunk@lightspeedsystems.com)
2023-07-12 - 4:05:30 PM CDT

Document e-signed by Gregory Funk (gfunk@lightspeedsystems.com)
Signature Date: 2023-07-12 - 4:05:45 PM CDT - Time Source: server

Agreement completed.
2023-07-12 - 4:05:45 PM CDT