

2025-2026 School Year

Dear WCSD Contractor,

In accordance with New York State Education Law §2-d, the District hereby implements the requirements of Commissioner's Regulations (8 NYCRR §121) requiring that any person or entity, other than an educational agency, that receives student data or teacher or principal data or staff data from an educational agency pursuant to a contract or other written agreement for purposes of providing services."

All products need to be vetted 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 Webster Central School District. The attached documentation is required to be completed for potential use of your product and/or contractor in accordance with New York State Education Law §2-d.

In order for us to verify that your product meets the requirements of Commissioner's Regulations (8 NYCRR §121), we will need the following information completed:

- Software agreement
- Data Security and Privacy Plan
- Parents' Bill of Rights-Supplemental Information Addendum

Please return this information to:

Brian Zimmer
110 Sanford Street
Webster, NY 14580
brian_zimmer@webstercsd.org

I am hoping that you may meet the criteria and would ask that if you have any questions please contact Brian Zimmer, Director of Educational Technology and Information/Data Protection Officer at brian_zimmer@webstercsd.org to further our abilities to use the program.

Sincerely,



Brian Zimmer
Director of Educational Technology and Information/Data Protection Officer
Webster Central School District
585-216-0099

WEBSTER CENTRAL SCHOOL DISTRICT SOFTWARE AGREEMENT-

Please complete entire document prior to review and acceptance.

This Agreement, made and entered into 09/01/2025 (Effective Date), by and between SLR Photography LLC, having offices at 1159 Pittsford Victor Road Pittsford NY 14534 ("Vendor"), and Webster Central School

District, having an office at 110 Sanford Street, Webster NY 14580 ("School District") (collectively "Parties").

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

x **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.

 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.

1. 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.

2. Term of Services. This Agreement begins on the Effective Date and will continue until terminated (the "Term").

3. 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.

4. Payment. Payment shall be made in accordance with Addendum C attached hereto.

5. 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.

6. 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.

7. 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.

8. Compliance with Laws. Vendor, its employees and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.

9. 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.

10. 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.

11. **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.

12. **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.

13. **Addendums.** The following Addendums are attached hereto and incorporated herein:

- Description of Specifications and Services
- Schedule of Data
- School District's Parents' Bill of Rights
- Parents' Bill of Rights – Supplemental Information Addendum
- Vendor's Data Security and Privacy Plan

14. **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.

15. **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.

Vendor

By: 
Name: Dina Mangiamiele
Title: Owner
Date: 9/15/2025

School District

By: 
Name: Brian Zimmer
Title: Director of Educational Technology
Date: 9/15/2025

DESCRIPTION OF SPECIFICATIONS AND SERVICES

Description of Services

School Photography and Yearbook Services

SCHEDULE OF

DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	
	Other application technology meta data (specify):	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): <i>Student Personality Assessments</i>	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information (specify):	
Enrollment	Student school enrollment	
	Student grade level	x
	Homeroom	x
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/Guardian Contact Information	Address	
	Email	x
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
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)	
Student Contact Information	Other indicator information(specify): <i>First Generation College Student</i>	
	Address	
	Email	
Student Identifiers	Phone	
	Local (School district) ID number	x
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
Student Name	Student app passwords	
	First and/or Last	x
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content, writing, pictures etc.	
	Other student work data (Please specify):	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	

Category of Data	Elements	Check if used by your system
	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 D

SCHOOL DISTRICT'S PARENTS' BILL OF RIGHTS

Webster Central School District Parents' Bill of Rights for Data Privacy and Security

The Webster Central School District is committed to ensuring student privacy in accordance with local, state and federal regulations and district policies. To this end and pursuant to U.S. Department of Education (DOE) regulations (Education Law §2-d), the district is providing the following Parents' Bill of Rights for Data Privacy and Security:

- A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes.
- Parents have the right to inspect and review the complete contents of their child's education record.
- State and federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls and password protection, must be in place when data is stored or transferred.
- A complete list of all student data elements collected by the state is available for public review both online and via regular mail from the New York State Department of Education (SED).
- Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Brian Zimmer, Director of Educational Technology and Information
Data Protection Officer
Webster Central School District
110 Sanford Street
Webster, NY 14580
Brian_zimmer@webstercsd.org
585-216-0099

And to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
cpo@mail.nysed.gov

The bill of rights is subject to change based on regulation of the Commissioner of Education and the SED Chief Privacy Officer. Changes/Additions are also anticipated as SED releases further guidance documents.

More information

If you would like more information, please contact Mr. Zimmer at 585-216-0099. More information is also available on the following websites:

- [New York State Department of Education guidance document](#) issued on July 29, 2014 (PDF)
- [U.S. Department of Education press release](#): Guidance for Schools Issued on How to Keep Parents Better Informed on the Data They Collect on Students (PDF)
- [Privacy Technical Assistance Center \(PTAC\)](#): newly established one-stop resource for education stakeholders to learn about data privacy.

DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Webster Central School District (hereinafter “School District”) and SLR Photography, LLC (hereinafter “Contractor”) entered into an agreement dated 9/1/2025 (hereinafter “Agreement”) for school photography and yearbook services (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):

We conduct regularly scheduled audits of our security software and hardware configurations to verify compliance. Including but not limited to antivirus and anti-intrusion software, hardware and software firewalls, and network policies restricting access and retention of sensitive data on our internal network

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:

We conduct regularly scheduled audits of our security software and hardware configurations to verify compliance. Including but not limited to antivirus and anti-intrusion software, hardware and software firewalls, and network policies restricting access and retention of sensitive data on our internal network

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

Training occurs monthly and is completed by the 10th of each month.

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:

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.

All data in transit over the internet is encrypted using TLS 1.2 or 1.3. Our internal network is protected from external access by modern anti-virus software, a hardware firewall, an application layer firewall and an encrypted VPN with two-factor authentication.

Laptops in the field (our highest-risk data environments) are encrypted and protected by a remote-wipe-capable technology, and data in transit from the field to the plant is encrypted transport

7. Termination of Agreement.

☒

Within **10** days of termination of the Agreement, Contractor shall delete all student data or teacher or principal data in its possession; AND within **10** days of termination of the Agreement, Contractor shall return all data to the School District using:

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. 9/1/2025_____.

CONTRACTOR

By:
Title:

**PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION
ADDENDUM-REQUIRED**

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 (the “Contractor”) are limited to the purposes authorized in the contract between the Contractor and Webster Central School District (the “School District”) dated (the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor 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 format and destroyed by the Contractor 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 Contractor’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 Contractor’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 Contractor by the School District will be stored
The measures that Contractor 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 Contractor 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.

NY State Privacy Policies from Inter-State Studio

Addendum E : Question 1 Exclusive Purposes for Data Use.

Services may include Student and Staff picture packages, Yearbook, Student and Staff ID Cards, banners, posters, and/or other related service items.

Addendum E : Question 3

Contract Practices

Data is purged from our systems at the end of the school year and is no longer accessible. PII data is deleted from all file storage, databases and backups within the time frames defined by our internal production policies and privacy agreement.

PII data is deleted from all file storage, databases and backups within the time frames defined by our internal production policies and privacy agreement.

Addendum E : Question 5

Security Practices

It depends on where data is in our workflow. Outside our hardened perimeter, it will be encrypted. Inside our hardened perimeter, it will be on storage devices password protected from unauthorized network access through directory rights management and/or 2FA.

Servers inside our perimeter are also physically protected from unauthorized access in our server room which is constructed with concrete walls and a steel vault style door. Limited access is granted only to required technology and safety staff.