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	Goodheart-Willcox Publisher _____
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	To facilitate data migration for an LMS or SSO/rostering integration.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 09/06/2023 Contract End Date 09/06/2026
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) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • 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.
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	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Goodheart-Willcox endeavors, within the constructs of its security practices, to ensure compliance with generally accepted security and privacy practices. Data is stored in a US-based Amazon datacenter. Amazon datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Encryption	Data will be encrypted while in motion and at rest.

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.	All parties who will deliver services as part of this Services Agreement are in alignment with EA's stated requirements. All parties follow a prevention, detection, and response strategy. All are responsible for complying with G-W's information security and privacy policies.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	G-W will work with the EA to minimize the data that is shared in order to provide the services. Access to EA data residing in Contractor's services is controlled through use of an access management and approval process and role-based access control.
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.	☐ Security and sensitive information awareness training ☐ Awareness and compliance with policy is part of the employment agreement ☐ In-house data breach plan for communicating with our customers and vendors ☐ Protect data in transit and at rest. ☐ Require Multi-Factor Authentication on administrator accounts
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.	G-W maintains technology rules of the road, privacy policy, and security awareness expectations and policies that are components of our employee agreements and onboarding process. We review and update those policies at most annually. G-W also maintains data protection, security of confidential information, and data breach terms and conditions in agreements with our Subcontractors.
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.	G-W services are designed to function with minimal PII to minimize risk of unintentional data exposure. When Contractor is made aware of a potential unauthorized disclosure of information from either its own employees and processes, its Subcontractors who monitor the network and systems, from the EA, or from another of Contractor's customers, Contractor initiates its internal process for improper data handling and data breach.Contractor will first notify the appropriate EA contact to provide information on the incident and support EA's procedures up to and including cobberation with authorities, investigation, and communication
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	G-W does not collect any grades, student data, or APPR data so no data transmission will be required upon the completion of services per this Services Agreement.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Once termination of an agreement is provided to G-W, or 60 days after the termination of the agreement upon written request from the EA, all EA data will be removed from G-W servers. G-W will provide notification to EA upon completion of the data destruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Maintain administrative, technical and physical safeguards to services. Maintain data security and privacy policies.Have processes to comply with data breach detection, investigation, and appropriate notification. Have processes to comply with data destruction upon termination of services.Encrypt data in transit and at rest.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	We have drafted our own internal processes in alignment with the NIST cybersecurity framework, and we attest to best practices compliance for our cybersecurity insurance renewals

Western Suffolk BOCES 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 should be submitted to: dpo@wsboces.org. (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]	Jennifer J. Selby
[Printed Name]	Jennifer J. Selby
[Title]	Sales Contracts and Proposals Manager
Date:	09/06/2023