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	Eduware Inc.
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 provide technical support to students, teachers, admins, and parentsfor TestWizard accounts. To provide teachers with an online assessment tool for student instruction.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 6/30/2022 Contract End Date 6/30/2025
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: Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies.
Encryption	Data will be encrypted while in motion and at rest.

DATA SECURITY AND PRIVACY PLAN

WHEREAS, Western Suffolk BOCES (hereinafter "School District") and Eduware, Inc. (hereinafter "Contractor") entered into an agreement dated 6/29/2022 (hereinafter "Agreement") for TestWizard.com, WizardTM.com, ClickerSchool.com (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):

(a) Eduware will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(b) Eduware will comply with the School District Data Security and Privacy Policy, Education Law §2-d, and 8 NYCRR §121.

(c) Eduware will limit internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services.

(d) Eduware will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.

(e) Eduware 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) Eduware will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.

(g) Eduware will use encryption to protect personally identifiable information in its custody while in motion or at rest.

(h) Eduware 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 Eduware engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Eduware shall apply to the subcontractor.

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:

(a) Server instances are isolated from public internet and only necessary ports are open for public access, there is no public IP address, if not needed.

- All instances are in configured AWS security groups, which means only specified ports are open to the internet and all management ports are closed.

(b) Operating systems have the latest security updates in order to prevent hacking attempts.

(c) SSL certificates are installed for all sites and all client communication will be encrypted.

(d) There are load balancer services in front of all production servers, which have built-in functions to prevent DDoS attacks.

(e) Database and other files are stored on password protected machines with HTTPS, firewall, and "login-gateway" to help keep data safe.

(f) AWS CloudTrail to save logs of AWS management events.

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 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*

(a) Company-wide FERPA and Security training was done April 1, 2020 and is done as necessary throughout the year and for new employees.

5. Subcontractors:

(a) Eduware, Inc. does not use subcontractors, however in the event that Eduware, Inc.engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Eduware, Inc. under the AGREEMENT and applicable state and federal law.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information:

(a) To immediately notify the School District in the most expedient way possible and without unreasonable delay and in no event more than seven (7) calendar days after discovering that any personally identifiable information of the School District, its employees, students, teachers, principals or administrators is breached and/or released without authorization;

(b) To take immediate steps to limit and mitigate to the greatest extent practicable the damages arising from any breach or unauthorized release of any personally identifiable information of the School District, its employees, students, teachers, principals or administrators;

7. Termination of Agreement.

(a) Upon expiration of this Contract without a successor agreement in place, the Vendor shall assist the School District in exporting all Protected Information previously received from, or then owned by the School District.

(b) Upon expiration of this Contract with a successor agreement in place, the Vendor will cooperate with the School District as necessary to transition protected data to the successor vendor prior to deletion. The Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of the Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of the Vendor in secure data center facilities.

(c) The Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 10/12/2020.

CONTRACTOR: Eduware, Inc.
Ingrid Hamilton
President, Eduware, Inc.

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.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
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.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
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.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please refer to Pages 3-6 document "DATA PRIVACY AND SECURITY PLAN"

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]	Shane Windt Digitally signed by Shane Windt Date: 2022.06.29 15:28:21 -04'00'
[Printed Name]	Shane Windt
[Title]	Sales Operations Manager
Date:	6/29/2022

January 13, 2022