TST BOCES
TOMPKINS • SENECA • TIOGA

Daniel Parker
Coordinator of Technology Services

555 Warren Road, Ithaca, NY 14850
607-257-1551, ext. 1016
dparker@tstboces.org

ADDENDUM A

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or Principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled STUDENT RECORDS: ACCESS AND INFORMATION DISCLOSURE;

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and

Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the TST BOCES District Privacy Officer; contact information can be found on the TST BOCES website;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

   - Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

   - Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;

   - The District will require complaints to be submitted in writing;

   - The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:

   - the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;

   - how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will 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., FERPA; Education Law §2-d);

- the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed);

- if and how a parent, student, eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;

- where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

ADDENDUM B

DATA PRIVACY RIDER FOR ALL CONTRACTS INVOLVING PROTECTED DATA PURSUANT TO EDUCATION LAW §2-C AND §2-D

District and Vendor agree as follows:

1. Definitions:

(1) Protected Data means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;

(2) Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Data shall be maintained in accordance with State and Federal Law and the District's Data Security and Privacy Policy;

3. The Parties agree that the District's Parents' Bill of Rights for Data Privacy and Security are incorporated as part of this agreement, and Vendor shall comply with its terms;

4. Vendor agrees to comply with Education Law §2-d and its implementing regulations;

5. Vendor agrees that any officers or employees of Vendor, and its assignees who have access to Protected Data, have received or will receive training on federal and State law governing confidentiality of such data prior to receiving access;

6. Vendor shall:

(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests;

(2) not use the education records for any other purposes than those explicitly authorized in its contract. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to a third party for marketing or commercial purposes;

(3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party:

(i) without the prior written consent of the parent or eligible student; or

(ii) unless required by statute or court order and the party provides notice of the disclosure to the department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

(5) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;

(6) adopt technology, safeguards and practices that align with NIST Cybersecurity Framework;

(7) impose all the terms of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Data.

Addendum C

Data Security & Privacy Plan

WHEREAS, the Tompkins Seneca Tioga BOCES (hereinafter "BOCES") and **C. W. Publications** (hereinafter "Contractor") entered into an agreement dated **1/1/2021** (hereinafter "Agreement") for **Cwpubonline** (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 BOCES.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the BOCES Data Security and Privacy Policy in the following way(s):
Please see attached documentation following your page 9

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:
Please see attached documentation following your page 9

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the BOCES 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 BOCES, 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 **Please see attached documentation following your page 9.**

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 BOCES.

7. Termination of Agreement.
a. Within 7 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 7 days of termination of the Agreement, Contractor shall return all data to the BOCES using **CSV*** ; OR Transition all data to a successor contractor designated by the School District in writing using **CSV***. ***Comma Separated Value**

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 **1/1/2021**.

BY THE VENDOR	BY THE BOCES
Signature	Signature
Charles R. Wilkinson	Daniel N Parker
Printed Name	Printed Name
President	Director of Information Technology Services
Title	Title
1/1/2021	9/22/2025
Date	Date

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

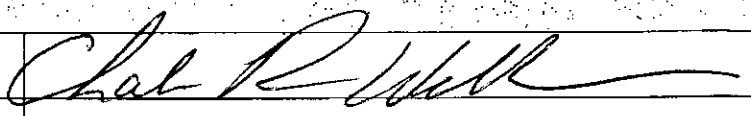
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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	**C. W. Publications**
Description of the purpose(s) for which Contractor will receive/access PII	**Student and teacher use of online educational software (cwpubonline)**
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII **Please see attached documentation following page 9 Our Student Data Collection and Usage (pages 2-3)** ☐ APPR Data
Contract Term	Contract Start Date **1/1/2021** Contract End Date **At the request of TST BOCES**

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: **Please see attached documentation following your page 9.** **Storage of Electronic Data (page 1)** **Physical Security Measures (page 2)**

Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	**C. W. Publications**
[Signature]	
[Printed Name]	**Charles R. Wilkinson**
[Title]	**President**
Date:	**1/1/2021**

C. W. Publications Privacy Policy

Your privacy is very important to us. Accordingly, we have developed this Policy in order for you to understand how we collect, use, communicate and disclose and make use of personal information. The following outlines our privacy policy.

- Before or at the time of collecting personal information, we will identify the purposes for which information is being collected.
- We will collect and use personal information solely with the objective of fulfilling those purposes specified by us and for other compatible purposes, unless we obtain the consent of the individual concerned or as required by law.
- We will only retain personal information as long as necessary for the fulfillment of those purposes.
- We will collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.
- Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.
- We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
- We will make readily available to customers information about our policies and practices relating to the management of personal information.
- We are committed to conducting our business in accordance with these principles in order to ensure that the confidentiality of personal information is protected and maintained.

Storage of Electronic Data:

Student data is stored in hashed format in an encrypted database. The only collected and stored data are student name, username, password (grade and email are optional). The information is only accessible to school personnel with a username and password to the admin portal.

Storage of Non-Electronic Data:

We do not collect or store non-electronic student data.

Personnel/Workforce Security Measures:

All personnel's identities are verified along with his/her right to work in the U.S. Confirmations are made regarding employment history and qualifications. All personnel are trained in the proper use of the company's electronic systems and only senior staff have access to systems that contain any student data.

Physical Security Measures:

All systems are run on servers located in a building that houses a secure date center. There is a biometric entry security for access into the building and separate biometric entry into the data center.

Account Management and Access Control:

C. W. Publications creates a single admin account for the school. That information is shared with the technical contact designated by the school. The school then creates accounts that adhere to the school's policy.

Our Student Data Collection and Usage

(Signified with a YES)

Application Technology Meta Data:	
IP Addresses, use of cookies, etc.	**YES**
Other Application technology meta data	No
Application Use Statistics:	
Meta data on user interaction with application	**YES**
Assessment:	
Standardized test scores	No
Observation data	No
Other assessment data	No
Attendance:	
Student school (daily) attendance data	No
Student class attendance date	No
Communications:	
Online communications that are captured (emails, blog entries)	No
Conduct:	
Conduct or behavioral data	No
Demographics:	
Date of birth, place of birth, gender, ethnicity or race, language information, other	No
Enrollment:	
Student school enrollment, student grade level, homeroom, guidance counselor	No
Specific curriculum programs, year of graduation, other	No

Parent/Guardian Contact Information:	
First and/or last name	No
Address, email, phone	No
ID number (created to link parents to students)	No
Schedule:	
Student scheduled courses and teacher names	No
Special Indicator:	
English language learner information	No
Low income status	No
Student disability information, medical alerts	No
Specialized education services	No
Living situations (homeless / foster care)	No
Student Contact Information:	
Address, email, phone	No
Student Identifiers:	
Local (school district) ID number	No
State ID number	No
Vendor/App assigned ID number	No
Student app username	**YES**
Student app passwords	**YES**
Student Name:	
First and/or last	**YES**
Student In-App Performance:	
Program/application performance	**YES**
Student Program Membership:	
Academic or extracurricular activities a student may belong to or participate in	No
Student Survey Responses:	
Student responses to surveys or questionnaires	No
Student Work:	
Student generated content, writing, pictures, etc	**YES**
Transcript:	
Student course grades	No
Student course date	No
Student course grades/performance scores	No