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	Coughlan Companies, LLC dba Capstone
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, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.
Description of the purpose(s) for which Contractor will receive/access PII	Contractor will receive/access PII to provide the requested Services to the District and perform the obligations under the Contract.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 07/01/2025 Contract End Date 06/30/2027
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: Capstone shall implement and maintain administrative, operational, and technical safeguards to protect Personally Identifiable Information (PII), in accordance with the NIST Cybersecurity Framework.
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.	Throughout the life of the contract: • A student's personally identifiable information cannot be sold or released for any commercial purposes • Parents have the right to inspect and review the complete contents of their child's education record • Contractor will follow state and federal laws which 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 will be in place when data is stored or transferred • Contractor will limit internal access to education records to those individuals that are determined to have legitimate educational interests • Except for authorized representatives of the Contractor to the extent they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior

		written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education 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 if expressly prohibited by statute or court order • Contractor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody • Contractor will use encryption technology to protect data while in motion or in its custody • Contractor will adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Only those who need it to perform their duties should have access to data • Training and guidance is provided to all employees that will be accessing and handling data (including more specifically, student data) • Background checks are performed on all employees • NDAs are signed by employees at the start of employment • All access to systems and data is revoked upon employment termination

- All data stored electronically is kept secure by taking the following precautions:
    - Use strong passwords that should never be shared
    - Servers are protected by security software and a firewall
    - Backup data frequently
    - Never disclose PII to unauthorized people within or outside of Capstone
    - Routinely monitor systems for security breaches and attempts of inappropriate access

Measures to Protect Data:
Capstone Digital Products use HTTPS connections to secure transmissions. A combination of firewalls, security keys, SSL certificates, and non-default username/password credentials secure data access. Additionally, Capstone Digital Products have preemptive safeguards in place to identify potential threats, manage vulnerabilities and prevent intrusion.

Capstone Digital Products use HTTPS connections to secure transmissions. The HTTPS you see in the URL of your browser means when you go to the website, you're guaranteed to be getting the genuine website. With HTTPS in place, all interactions with Capstone Digital Products will be undecipherable by an outside observer. Capstone Digital Products use SSL security at the network level to ensure all information is transmitted securely.

Account information is stored in access-controlled VPCs operated by industry leading partners. All user information is stored redundantly and backed up in geographically distributed data centers.

		We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner. Capstone Digital Products are hosted on cloud servers managed by Amazon Web Services which is compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption.
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.	Officers and all employees of the Contractor who have access to student, teacher or principal data will receive ongoing training surrounding the Federal and State laws governing confidentiality of the data. This training will be performed and tracked through Curricula.
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.	All Third-Party Vendor Agreements and District Service Agreements must go through the Contracts, Compliance, and Data Privacy department to negotiate and agree to the privacy and service terms throughout the life of the contract. All Third-Party Vendors are also vetted by the Information Technology department to ensure that they abide by the same data security policies as the Contractor. 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 Service Agreement.
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.	Capstone has implemented the following procedure to manage a data breach: Breach Investigation: A systematic approach to making a definitive determination as to whether a breach has taken place is led by the Incident Response Team to investigate a potential breach. The response team will be tasked with isolating the affected systems, including taking the part or the

		entire site offline. Remediation Efforts: Upon identification, the response team will review the access logs and the monitoring software to figure out the cause of the breach. We will also consult experts at the cloud hosting service providers to help with the issue. Once the cause is identified, we will apply and monitor the fix and gradually bring the site online. The response team will also reset all session tokens for its users which will require that they log in again. Access tokens are valid for 24 hours in order to prevent unauthorized access. Internal Communication Plan: If it has been determined a breach occurred, the response team will inform the President and explain what is being done to remediate the issue. After a solution has been implemented, an incident report detailing the cause, extent of damage, steps taken and recommendations to avoid in the future will be written by the response team and shared internally. Public Notification of Breach: After remediating the issue, the marketing team will work on informing all affected users about the breach and its severity. A brief statement will be shared via email explaining the incident and the solution will be sent after remediation is finalized. Additionally, the response team will monitor the dedicated email address privacy@capstonepub.com to address any follow-on questions.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon written request of EA, Contractor shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Contractor acknowledges EA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by EA. Nothing in the Service Agreement shall authorize Contractor to maintain Data

		obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to EA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been deidentified or placed in a separate Student account, pursuant to the other terms of the Service Agreement.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon written request of EA, Contractor shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to EA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been deidentified or placed in a separate Student account, pursuant to the other terms of the Service Agreement
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will comply with the EA's applicable policies and Education Law section 2-d by adhering to the following guidelines: • A student's personally identifiable information cannot be sold or released for any commercial purposes • Parents have the right to inspect and review the complete contents of their child's education record • Contractor will follow state and

		federal laws which 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 will be in place when data is stored or transferred • Contractor will limit internal access to education records to those individuals that are determined to have legitimate educational interests • Except for authorized representatives of the Contractor to the extend they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education 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 if expressly prohibited by statute or court order • Contractor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its

		custody • Contractor will use encryption technology to protect data while in motion or in its custody • Contractor will adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework Contractor has also documented the following information regarding the receipt of student, teacher or principal data: • The exclusive purposes for which the student data or teacher or principal data will be used. • How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, will abide by data protection and security requirements. • When the agreement expires and what happens to the student, teacher or principal data upon expiration of the agreement. • 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, teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	**Identify (Asset Management, Risk Assessment, Governance)** • Maintain a current data inventory of all data collected • Classify data according to sensitivity • Perform periodic risk

assessments focused on K–5 use cases

- Define roles and responsibilities for safeguarding student information

Protect (Access Control, Data Security, Awareness Training)

- Enforce role-based access control so only authorized educators/admins/employees have access to data
- Apply encryption in transit and at rest for all PII
- Provide single sign-on (SSO) / secure authentication compatible with school identity providers
- Provide privacy training to employees, as well as user guidance for schools and districts
- Limit data retention to what is educationally necessary

Detect (Anomalies, Monitoring, Continuous Security)

- Use logging and monitoring to detect unusual login activity or unauthorized data access
- Perform regular vulnerability scanning and penetration testing of systems
- Monitor third-party integrations for compliance with our data-handling standards

Respond (Incident Response Planning, Communication)

- Maintain a documented incident response plan aligned with state student data privacy laws
- Define clear escalation paths for suspected breaches, including notification procedures for schools and districts
- Commit to timely notification of impacted educational institutions if a data event occurs

Recover (Recovery Planning, Improvements)

- Implement tested backup and restore processes to ensure

		continuity of learning • Conduct post-incident reviews to improve security and privacy practices • Share lessons learned with stakeholders

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]	Eric Helgason
[Printed Name]	Eric Helgason
[Title]	EVP of Finance and Operations
Date:	08/20/2025