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 contractorsthat will receive Personally Identifiable Information (PII).

Name of Contractor	Turnitin, LLC
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Yes 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 socialsecurity 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	Our products process personal and institutional data to support core functionality, ensure academic integrity, enhance user experience, and improve our services. This includes information such as name, email address, and institution name, as well as technical identifiers like IP address, device ID, browser type, and interactions with our services. In some cases, we may also process user-submitted content (e.g., assignments, exams, or feedback) as part of our services. We collect and use this data in accordance with our privacy policy and contractual agreements. Please reference the Turnitin Privacy Policy: https://guides.turnitin.com/hc/en-us/articles/27377195682317-Turnitin-Services-P

	rivacy-Policy#Personal_Information
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR PII

Contract Term	Contract Start Date: 01 September 2025 Contract End Date: 31 August 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. Turnitin's Technical Services team can assist customers with exporting their data upon the conclusion of their Turnitin Feedback Studio license. The service provides copies of the indexed original submitted documents along with associated metadata (student, class assignment, similarity score, grade if added) in the format detailed below (Metadata CSV File Structure section). Unindexed content is not included on the basis that it is not used for matching on the Turnitin service, so should not be used for matching in the service ingesting the documents. • Securely delete and destroy data. The data is removed via AWS API calls to services hosting the data, and AWS assures customers that it uses industry-standard secure data deletion practices.
Challengesto 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. Please reference the Turniti Privacy Policy: https://guides.turnitin.com/hc/en-us/articles/27377195682317-Turnitin-Services-Privacy-Policy#Personal_Information

Secure Storage and Data Security	Please describe where PII will be stored and the protectionstaken 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: Turnitin maintains Information Security and Risk Management policies to define how security vulnerabilities are identified, remediated, or mitigated based on risk severity level. Critical-level vulnerabilities shall be remediated or mitigated within 30 days. Turnitin responds actively and aggressively to any widespread industry security events. General system-level security enhancements not tagged as critical by the vendors are evaluated monthly in line with our system testing and quality assurance activities to ensure general patches do not cause software problems on our platform. Turnitin regularly performs vulnerability scans of our infrastructure in addition to annual third-party penetration tests to proactively identify vulnerabilities or security weaknesses. Remediation of vulnerabilities or security weaknesses identified in either third-party penetration tests or vulnerability assessments is addressed in accordance with the Company's vulnerability management policies. Attestation letters for the results of the latest penetration tests can be provided upon a specific written request and require an NDA to be in place.
Encryption	Data will be encrypted while in motion and at rest. Turnitin uses industry-standard technologies to encrypt data both in transit and at rest. For data in transit, Turnitin forces HTTPS and at minimum TLS 1.2 on all internet traffic. Data at rest are encrypted with at minimum AES-256 bit encryption.

~~Western Suffolk BOCES - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN~~

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 addressesits 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, contractorsshould 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 reference the Turniti Privacy Policy: https://guides.turnitin.com/hc/en-us/articles/27377195682317-Turnitin-Services-Privacy-Policy#Personal_Information
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Turnitin follows software development and coding standards that address security throughout the software development life cycle. Products are developed in accordance with the Agile Software Development Framework. Software development activities are subject to Turnitin's Change Management Policy. Turnitin aligns with the principle of least access privilege to govern permissions to codebase, infrastructure, and applications.
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.	Turnitin has implemented formal HR processes, including background checks, code of conduct and signed non-disclosure agreements as part of its onboarding process. Security awareness training is conducted up onboarding and once annually thereafter.
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 reference the Turnitin Data Process Agreement: https://www.turnitin.com/dpa
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.	Turnitin has a documented procedure for identifying, assessing, and treating privacy risks and opportunities for improvement.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Turnitin's Technical Services team can assist customers with exporting their data upon the conclusion of their Turnitin Feedback Studio license. The service provides copies of the indexed original submitted documents along with associated metadata (student, class assignment, similarity score, grade if added) in the format detailed below (Metadata CSV File

		Structure section). Unindexed content is not included on the basis that it is not used for matching on the Turnitin service, so should not be used for matching in the service ingesting the documents.
7	Describe your secure destruction practices and how certification will be provided to the EA.	The data is removed via AWS API calls to services hosting the data, and AWS assures customers that it uses industry-standard secure data deletion practices.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please reference the Turnitin Feedback Studio Security Package.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Turnitin's Information Security function is comprised of an experienced and dedicated team of engineers and analysts, led by the Senior Director, Security and Compliance. The team is responsible for identifying, assessing, and mitigating cybersecurity and compliance risks across Turnitin. The development and enforcement of security policies, processes and best practices within Turnitin is managed by this team. Turnitin has implemented a risk based security strategy based on NIST CSF that applies the principles of Defense-in-Depth into the protection of our data, products, clients and employees. .

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents(including legal guardians or personsin 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 identifierssuch 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'sidentity. 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'sidentifiable information.

4. Safeguards associated with industry standards and best practicesincluding, 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) Complaintsshould 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 regulationsif 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 practicesthat protect PII.

9. Educational agency contracts with vendorsthat receive PII will addressstatutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	DocuSigned by: 705FC2A8E9CC45B...
[Printed Name]	Angela Rhee
[Title]	Sr. Director Business Affairs
Date:	Aug-13-2025 | 08:27 PDT

March 12, 2024