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	PTC Inc. dba Onshape _____
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. 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 the Onshape SaaS service and to validate compliance
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

PDFfiller Document ID: 61F4-7E50-2AE1-0000

Contract Term	Contract Start Date 10/26/2026 Contract End Date 10/27/2031
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:
Encryption	Data will be encrypted while in motion and at rest.

PDFfiller Document ID: 61F4-7E50-2AE1-0000

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.	PTC/Onshape is a global company. We adhere to the rigorous standards of state, federal and applicable EU laws. Onshape's security team is comprised of: offensive (red team) engineers, defensive (blue team) engineers, and compliance experts. Onsh
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	1. TLSv1.2 encryption of all information in motion 2. AES-256 encryption of all data at rest 3. A SOC 2, Type II report describing the correct design and operational effectiveness of internal controls related to the secur
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.	As part of its Compliance program PTC/Onshape requires that all employees and contractors to be trained on data protection security and confidentiality standards and regulations on hiring as part of the onboarding process, and 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.	All PTC employees and sub-contractors are legally bound to preserve the confidentiality of any personal information that they have access to in the course of their employment/ engagement with PTC. PTC/Onshape trains its employees who have access to personal information on maintaining confidentiality and data security in compliance with applicable state and federal laws. As
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.	PTC's technical and organizational data security measures comply with industry standards and PTC will follow its data incident response plan to mitigate the impact of any data incident on any affected school or individual. PTC's data incident response policy requires those affected by an incident to be notified, via e-mail, without undue delay of PTC becoming aware of the incident.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon request of the EA, PII will be returned via text files and student content will be returned via CAD format.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will remain in Onshape backups subject to our retention and deletion policies here: https://www.onshape.com/en/privacy-center/privacy-policy
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor has (a) designated an employee to coordinate its information security program, (b) identified reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of School District's Information that c
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	PLEASE SEE BELOW .

Additional Information (More information can be provided at the bottom 2 pages):

PDFfiller Document ID: 61F4-7E50-2AE1-0000

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]	Erin Christenson Signed • Oct 26, 2026
[Printed Name]	Erin Christenson
[Title]	Sr. Corp Counsel
Date:	10/26/2026

Version: 4/30/25

PDFfiller Document ID: 61F4-7E50-2AE1-0000

Additional Information:

1 Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract. PTC/Onshape is a global company. We adhere to the rigorous standards of state, federal and applicable EU laws. Onshape's security team is comprised of: offensive (red team) engineers, defensive (blue team) engineers, and compliance experts. Onshape works with PTC's Chief Data Privacy Officer to follow all applicable laws.

2 Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. 1. TLSv1.2 encryption of all information in motion
2. AES-256 encryption of all data at rest
3. A SOC 2, Type II report describing the correct design and operational effectiveness of internal controls related to the security, availability, and confidentiality of the Onshape service.

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. As part of its Compliance program PTC/Onshape requires that all employees and contractors to be trained on data protection security and confidentiality standards and regulations on hiring as part of the onboarding process, and 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.
All PTC employees and sub-contractors are legally bound to preserve the confidentiality of any personal information that they have access to in the course of their employment/ engagement with PTC. PTC/Onshape trains its employees who have access to personal information on maintaining confidentiality and data security in compliance with applicable state and federal laws. As part of its selection and onboarding process for vendors/subcontractors, PTC/Onshape reviews their technical and organizational measures security and privacy measures, performs appropriate data protection impact assessments, where necessary, and enters into data protection addendum agreements with those who will have access to personal information.

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. PTC's technical and organizational data security measures comply with industry standards and PTC will follow its data incident response plan to mitigate the impact of any data incident on any affected school or individual. PTC's data incident response policy requires those affected by an incident to be notified, via e-mail, without undue delay of PTC becoming aware of the incident.

6 Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. Upon request of the EA, PII will be returned via text files and student content will be returned via CAD format.

7 Describe your secure destruction practices and how certification will be provided to the EA. PII will remain in Onshape backups subject to our retention and deletion policies here: https://www.onshape.com/en/privacy-center/privacy-policy

8 Outline how your data security and privacy program/practices align with the EA's applicable policies. Contractor has (a) designated an employee to coordinate its information security program, (b) identified reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of School District's Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessed the sufficiency of any safeguards in place to control these risks, and (c) designed and implemented information safeguards to control the risks identified through the risk assessment, and regularly tests or otherwise monitors the effectiveness of safeguards' key controls, systems and procedures. Contractor conducts periodic risk assessments and remediates any identified security vulnerabilities in a timely manner.
Contractor also has an incident response plan, which includes prompt notification to the School District in the event of a security or privacy incident, as well as best practices for responding to a breach of PII.

9 Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below. PLEASE USE TEMPLATE BELOW.

PDFfiller Document ID: 61F4-7E50-2AE1-0000

Additional Information:

PDFfiller Document ID: 61F4-7E50-2AE1-0000