

Onshape Student Data Privacy Addendum

This Onshape Student Data Privacy Addendum (the "Addendum") is attached to and forms a part of the Onshape Terms of Use and Privacy Policy (found here: <https://www.onshape.com/legal/terms-of-use>) for the provision of Onshape Education (the "Agreement") between PTC Inc., acting through its Onshape business unit ("Onshape") and the Educational Agency or Institution ("Customer").

1. **Purpose:** The purpose of the Addendum is to describe the duties and responsibilities of Onshape to protect Student Data transmitted by Customer to Onshape pursuant to the Agreement for Onshape Education or created by Students in the use of the Onshape Service, including compliance with all applicable statutes for the protection of student privacy and confidentiality, including the Family Educational Rights and Privacy Act.
2. **Definitions:** Unless expressly defined in the Agreement, all capitalized terms not defined herein shall have the meaning ascribed to it by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g ("FERPA")

"Student Data" means Records, Directory Information and Personally Identifiable Information (PII) or data that is linked to information or material that personally identifies an individual, any information directly related to a Student that is maintained by a local or regional board of education, the State Board of Education or the Department of Education or any information acquired from a Student through the use of the Service. "Student Data" does not include de-identified Student information used to (a) improve educational products for adaptive learning purposes and customize Student learning, (b) demonstrate the effectiveness of Onshape products in the marketing of such products, and (d) develop and improve the Services.

3. **Onshape Service:** Onshape Education is a version of PTC Inc's Onshape SaaS CAD service that has been developed for use in K-12 schools and universities. Onshape Education is the only fully online, cloud-based CAD system that enables remote learning and instruction. Onshape Education runs on all computers, tablets and mobile devices. Onshape is built for virtual teams and allows real-time collaboration for students and teachers.
4. **Student Data:** The categories of Student Data processed by Onshape in the provision of Services includes, but is not limited to:
 - a. PII, alias, usernames, IP addresses, email addresses;
 - b. Interactions with the Onshape service;
 - c. Data relating to the location of the user based on IP address;
 - d. School and Education Records; and
 - e. Records of certifications with the Service.
5. **Rights to Student Data:** All Student Data remains the property of Customer or that eligible Student. Onshape has a limited, nonexclusive license to Student Data solely for the purpose of performing its obligations under the Agreement. Onshape shall not use Student Data for any targeted advertising. Onshape shall not sell Student Data or share Student Data except as required under the terms of the Agreement for the provision of the Services.

6. **Access to and Deletion of Student Data:** Customer, a Student or Parent may request access to or the deletion of Student Data by submitting a request for deletion to Onshape by electronic mail to privacy@onshape.com. Onshape will provide details of all applicable Student Data or delete the Student Data (as appropriate) within ten (10) business days of receiving such request. Onshape's obligation to delete Student Data shall not apply in instances where such Student Data is (a) otherwise prohibited from deletion or required to be retained under State or Federal law, or (b) stored as a copy as part of a disaster recovery storage system and that is (i) inaccessible to the public, and (ii) unable to be used in the normal course of business by Onshape.

Onshape shall dispose or delete all Student Data obtained under the Agreement when it is no longer needed for the purpose for which it was obtained. On Customer's request Onshape shall provide written confirmation to Customer when the Student Data has been deleted.

7. **Correcting Erroneous Student Data:** Customer, a Student or Parent may review Personally Identifiable Information contained in Student Data and correct any erroneous information, if any. Onshape agrees to reasonably cooperate with Customer to permit a Student or Parent to review and correct any erroneous Personally Identifiable Information contained in Student Data that has been previously provided to Onshape.

8. **Onshape Employees:** Onshape shall ensure that its employees and all subcontractors, agents, representatives who have access to Student Data have a) undergone appropriate background screening and possess all needed qualifications to comply with the terms of this Addendum and b) have received or will receive appropriate training concerning the handling of Student Data to protect its confidentiality and privacy, such training being in compliance with Federal and State Law concerning access to Education Records.

9. **Security:** Onshape maintaining administrative, physical and technical safeguards to protect Student Data in accordance with NIST Cybersecurity Framework, including but not limited to, encryption, firewalls, and password protection. Onshape maintains a SOC 2 Type II report which is externally audited on a regular basis. A copy of this report is available under NDA by request. Onshape's Data Security and Privacy Plan are attached to this Addendum.

10. **Security Breach:** In the event of Onshape becoming aware of any actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data ("Security Breach"), Onshape shall notify Customer in writing without undue delay, and in any event within 48 hours. The Security Breach notification shall include the following information:

- *What Happened:* describe the nature of the Security Breach and the likely consequences of the Security Breach
- *What Information was involved:* details of the Student Data concerned;
- *What steps are being taken:* describe the measures taken or proposed to be taken by Onshape to address the Security Breach and to mitigate its effects.
- *Where more information can be obtained:* provide the name and contact details of the Onshape contact point where more information concerning the Security Breach can be obtained;

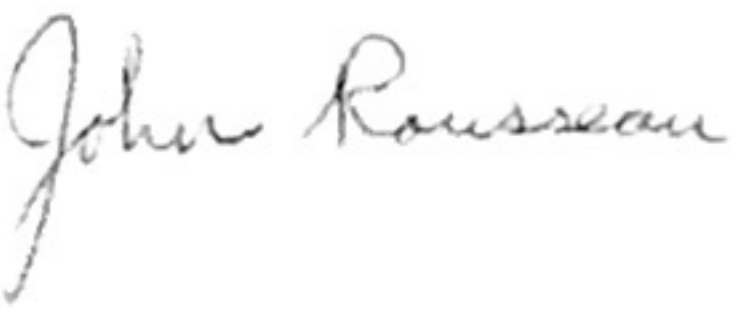
If the above information is not immediately available, Onshape shall provide such information when available. Onshape shall not make any public statement identifying Customer as an affected party, nor provide any official notification to any regulatory authority on behalf of Customer, without obtaining Customer's prior written consent.

11. **Compliance with Applicable Laws:** Onshape and Customer shall each ensure their own compliance with FERPA, the Children's Online Privacy and Protection Act, 16 CFR Part 312 ("COPPA"), and all other applicable State and Federal laws, as amended from time to time. Where applicable, the Parents' Bill of Rights for Data Privacy and Security (<https://www.onshape.com/legal/new-york-parents-bill-of-rights.pdf>) in accordance with New York State Education Law is incorporated by reference.

12. **Termination:** This Addendum will remain in effect until Customer subscription is terminated in accordance with the Agreement. Student Data shall not be retained or available to Onshape upon expiration of the Agreement, except a student, Parent or legal guardian of a student may choose independently to establish or maintain an electronic account with Onshape after the expiration of the Agreement for the purpose of storing Student Generated Content.

13. **Miscellaneous:** The parties agree that Addendum controls over any inconsistent terms or conditions contained within the Agreement.

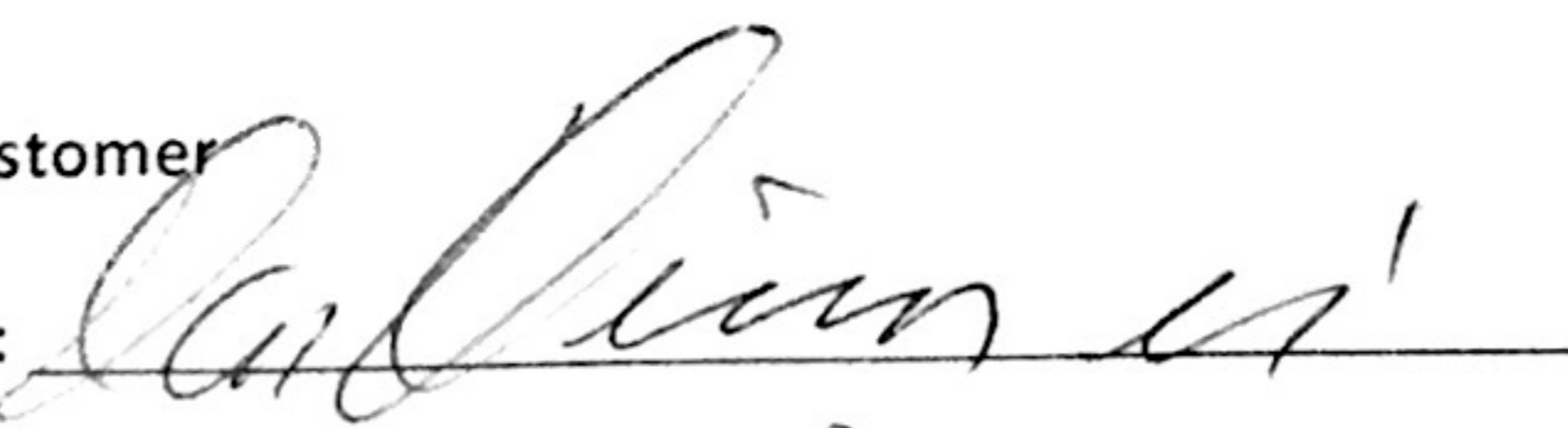
PTC Inc., acting through its Onshape business unit ("Onshape")

By: 

Date: August 31, 2020

Printed Name: John Rousseau

Title: VP, Technical Operations, Onshape

Customer
By: 

Date: 12/18/2020

Printed Name: Dan Davison Jr

Title: DPD

Onshape Data Security and Privacy Plan

VENDOR	PTC Inc., acting through its Onshape business unit
PRODUCT	Onshape Education
COLLECTS STUDENT DATA	<ul style="list-style-type: none"> a. Real names, alias, usernames, IP addresses, email addresses; b. Interactions with the Onshape service; c. Data relating to the location of the user based on IP address; d. School and Education Records; and e. Records of certifications with the Service.
Exclusive Purpose for use of Student Data; Description of Onshape Education	Onshape Education is a version of PTC Inc's Onshape SaaS CAD service that has been developed for use in K-12 schools and universities. Onshape Education is the only fully online, cloud-based CAD system that enables remote learning and instruction. Onshape Education runs on all computers, tablets and mobile devices. Onshape is built for virtual teams and allows real-time collaboration for students and teachers.
Subcontractors	Apart from PTC Inc's wholly owned affiliates, no sub-contractors are used in the delivery of the Onshape Education Service. All of PTC's Affiliates are bound to adhere to terms similar to those set out in this Agreement and Privacy Addendum.
Agreement Lifecycle Practices	The Agreement expires in accordance with its terms (see https://www.onshape.com/legal/terms-of-use) and section 6 above. When the Agreement expires or is terminated, Student Data will be deleted by Onshape, in accordance with the terms of the Agreement and this Addendum.
Onshape Contact Details	To access Student Data or request its deletion, a student, parent or legal guardian of a student or eligible teacher may contact Onshape via email at: privacy@onshape.com Onshape may ask for information to verify the identity of the requester and their relationship with the Student.
Security Practices	Security protections that align with the NIST Cybersecurity Framework are taken to ensure Student Data will be protected. Onshape has achieved a SOC 2, Type II certification using the AICPA's Trust Service Criteria for security, availability and confidentiality. A copy of Onshape's SOC 2 report is available under NDA. For more information concerning Onshape Security, please see https://www.onshape.com/security The Onshape Service is hosted on servers located in Oregon, USA (AWS West 2 Region) for Customers accessing the Service from the US. All data between client devices and the Onshape service is encrypted with TLS v1.2 using strong cipher suites. All data at rest is encrypted with the AES-256 encryption standard in XTS mode with keys managed by the AWS Key Management System.

THIRD-PARTY CONTRACTS CHECKLIST

Select one district software platform and work with colleagues to populate information from the related contract into the third-party contracts' checklist.

VENDOR:	PTC	PRODUCT:	OnShape
CONTAINS:	<input checked="" type="checkbox"/> Student Data	<input type="checkbox"/> Teacher or Principal Data	
REVIEW BY:	Dan Davison Jr.	REVIEWED DATE:	12/8/2020

It is highly recommended that the reviewer attach related agreements to this checklist. Use Tables 1 and 2 to populate information related to the statutory requirements that must be addressed in each contract.

CONFIDENTIALITY REQUIREMENTS	2-D	121	Y	N	WHAT SECTION?
Is there a provision that confidentiality of the shared data be maintained in accordance with federal and state law?	5(d)	2(c)	✓		9
Is there a provision that confidentiality of the shared data be maintained in accordance with the district/BOCES Policy on Data Security and Privacy?	5(d)	2(c)	✓		9

DATA SECURITY AND PRIVACY PLAN REQUIREMENTS	2-D	121	Y	N	WHAT SECTION?
Is there a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the district/BOCES Policy on Data Security and Privacy?	5(e)	6(a)	✓		9,10
Does the plan specify the administrative, operational and technical safeguards and practices the contractor has in place to protect personally identifiable information?		6(a)	✓		9
Does the plan demonstrate compliance with the supplemental information requirements (see Table 3)?		6(a)	✓		
Does the plan specify how the vendor's officers and employees who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access?	5(e)	6(a)	✓		8
Does the plan specify how the vendor's assignees (subcontractors) who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access?	5(e)	6(a)	✓		8
Does the plan specify if the contractor uses subcontractors and how it will manage any relationships and contracts to ensure personally identifiable information is protected?		6(a)	✓		8,9
Does the plan specify how the contractor will manage data security and privacy incidents, identify breaches and unauthorized disclosures, and promptly notify the agency?		6(a)	✓		10
Does the plan specify whether, how and when data will be returned to the agency, transitioned to a successor contractor, or destroyed by the contractor when the contract is terminated?		6(a)	✓		6
Does the plan include a signed copy of the district/BOCES Parents Bill of Rights for Data Privacy and Security?	5(e)			✓	

THIRD-PARTY CONTRACTS CHECKLIST

Use Table 3 to populate information the district/BOCES needs to post about the contract (supplemental information) with the Bill of Rights for Data Privacy and Security.

SUPPLEMENTAL INFORMATION ELEMENT	2-D 121		SUPPLEMENTAL INFORMATION
The exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract	3(c)	3(c)	
How the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract	3(c)	3(c)	
When the agreement expires and what happens to the protected data when the agreement expires	3(c)	3(c)	
If a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how	3(c)	3(c)	
Where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated	3(c)	3(c)	
How the data will be protected using encryption.	3(c)	3(c)	

THIRD-PARTY CONTRACTS CHECKLIST

Use Table 4 to populate information about other contract considerations relevant to Education Law 2-d and general contractual best practices.

CONTRACT CONSIDERATION	2-D	121	Y	N	WHAT SECTION?
Includes language that requires the vendor to provide notice of breaches and unauthorized disclosures of protected data in accordance with the Commissioner's Regulations (no more than 7 days after discovery).	6(a)	10(a)	✓		10
Includes language that tracks the statutory requirements imposed on vendors by Section 2-d, subsection 5(f) and the related regulations: <ul style="list-style-type: none"> • Vendor will adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework; • Vendor will comply with the data security and privacy policy of the district/BOCES, Education Law Section 2-d, and Part 121 of the Commissioner's Regulations; • Vendor will limit access to education records to persons with a legitimate educational interest; • Vendor will not use education records for any purposes other than those explicitly authorized in the contract; • Vendor will not disclose PII to any other person (except a person authorized by the vendor to help carry out the contract) without consent of the parent or eligible student, unless required to do so by statute or court order and the educational agency has been given notice of the disclosure; • Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII student information; • Vendor will use encryption technology to protect data in motion and data at rest using a technology or methodology specified in guidance issued by the U.S. Secretary of Health and Human Services to implement HIPAA. • Vendor will not sell PII nor use or disclose it for any marketing or commercial purpose, and will not facilitate the use or disclosure of PII by any other party for any marketing or commercial purpose, and will not permit any other party to do so; and • If Vendor engages a subcontractor to perform its contractual obligations, it shall ensure that the subcontractor is contractually bound to comply with the same data protection obligations imposed on the Vendor by state and federal law and this contract. 					
		9(a)	✓		9
		9(a)		✓	
	6(f)	9(a)	✓		6
	6(f)	9(a)	✓		8
	6(f)	9(a)	✓		8
	6(f)	9(a)	✓		8
	6(f)	9(a)	✓		9
		9(a)	✓		5
		9(b)	✓		9

The contract is governed by New York State law without regard to the state's choice of law rules, and venue is in the District's county and federal court district.			✓		11
Indemnification language is bilateral, not merely requiring the District to indemnify the vendor.					
Price increases capped.					



This resource is relevant to the THIRD-PARTY CONTRACTS Part 121 of the Commissioner's Regulations Requirements.