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.	Contractor will employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. Please see Contractor's Security Whitepaper for more details: https://code.org/about/InformationSecurityPolicy.pdf .
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See above.
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.	Contractor will provide annual privacy and security awareness training to those of its employees who operate or have access to the Services. This will include training on federal and state laws governing the confidentiality of Student Data.
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.	Contractor requires all employees and agents who have access to Student Data to comply with all applicable provisions of Ed Law 2-d and will require an appropriate confidentiality agreement from each employee or agent with access to Student Data.
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.	Contractor maintains an incident response plan. Security incidents are managed by a combination of the Chief Technology Officer, Privacy Counsel, and the Leadership team. Provider shall provide notification of any breach affecting Student Data to LEA as required by the applicable state law, and in the most expedient way possible and without unreasonable delay, but in no event later than seven (7) calendar days 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.	Contractor will, at the District's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable period following a written request. If no written request is received, Contractor will dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Contractor will not delete or destroy data for accounts where a student has established a personal login to be able to retain access and control over the student's own Student Generated Content.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or De-Identified. At the District's request, Contractor shall provide written notification to LEA when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor aligns its data security practices related to Student Data to the NIST Cybersecurity Framework. Please see Contractor's Security Whitepaper for more details: https://code.org/about/InformationSecurityPolicy.pdf .
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Contractor aligns its data security practices related to Student Data to the NIST Cybersecurity Framework.

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	Code.org
Description of the purpose(s) for which Contractor will receive/access PII	Code.org is a nonprofit dedicated to expanding participation in computer science by making it available in more schools, and increasing participation by women and underrepresented students of color. Code.org provides its computer science platform and curriculum without charge and will receive/access PII for the sole purpose of maintaining student accounts and progress in connection with the platform.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date: Term begins with creation of teacher account(s) to use platform in accordance with the Code.org Terms of Service at https://code.org/tos. Contract End Date: Term ends upon termination by either party as set forth in the Terms of Service and deletion of all teacher accounts.
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. Code.org's list of subcontractors is published from a link in the Code.org Privacy Policy at https://code.org/privacy and can be found here: https://docs.google.com/spreadsheets/d/e/2PACX-1vQ_AYYT_4K9Hpc5LrL4QAeXUmEMQR7rAXrHtloM4yt3xNndqPh-ABHXy0SJHZQ8ZSDSFQQv7ZWdXQjj/pubhtml?gid=222345124&single=true
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. If no written request is received, Contractor shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Code.org will not delete or destroy data for accounts where a student has established a personal login in order to be able to retain access and control over the student's own Student Generated Content.
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: All Student Data associated with Code.org accounts is stored on AWS servers in the United States. Contractor agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. Please see Contractor's Security Whitepaper for more details: https://code.org/about/InformationSecurityPolicy.pdf .
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	DocuSigned by: Cameron Wilson FD2D85824BA6481
[Printed Name]	Cameron Wilson
[Title]	COO
Date:	9/1/2021 | 13:05:18 PDT

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]	DocuSigned by: Cameron Wilson ED2D85824BA6481...
[Printed Name]	Cameron Wilson
[Title]	COO
Date:	9/1/2021 | 13:05:18 PDT