


## EXHIBIT A - 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](http://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 the EA at: CA BOCES Data Privacy Officer, 1825 Windfall Road, Olean, New York 14760, via email at [DPO@caboces.org](mailto:DPO@caboces.org) or by using the form available at the following website: <https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/>.
  - (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://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](mailto: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:	
Printed Name:	
Title:	
Date:	

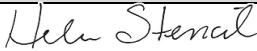
## EXHIBIT B

### 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).

<b>Name of Contractor</b>	
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date _____ Contract End Date _____
<b>Subcontractor Written Agreement Requirement</b>	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) <input type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>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.</li> <li>Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	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.

<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
<b>Encryption</b>	<p>Data will be encrypted while in motion and at rest.</p>

<b>CONTRACTOR</b>	
<b>Signature:</b>	
<b>Printed Name:</b>	
<b>Title:</b>	
<b>Date:</b>	

## EXHIBIT C - 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 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.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	
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.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
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.

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional

Function	Category	Contractor Response
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	

Function	Category	Contractor Response
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	

Function	Category	Contractor Response
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	



## **NOCTI Data Sharing Policy**

Safeguarding the confidentiality of individual personal information is the responsibility of all organizations and individuals who collect, maintain, access, transfer, or use education or training records. Under the Family Educational Rights and Privacy Act (FERPA), 34 CFR § 99.31(a)(1)(i), NOCTI is provided access to students' personally identifiable information (PII) to deliver agreed-upon assessment services to its student testing customers. NOCTI takes privacy seriously and makes every effort to protect disclosure of PII for all customers.

NOCTI has rigorous security systems and processes in place for the specific purpose of protecting all assessment-related data (ARD). ARD includes PII related to assessment login procedures, scoring, timing, pre-tests, re-takes, and any accompanying education or training records in the form of disaggregated score results.

This policy establishes the general guidelines NOCTI follows with respect to data sharing. Independent data sharing agreements with collaborative organizations or agencies may be signed to outline specific data handling practices and to ensure adherence to this guiding policy.

### **Data Sharing**

NOCTI will:

1. Establish and use appropriate administrative, technical, and physical safeguards to store and protect ARD from being accessed, used, or disclosed to unauthorized parties.
2. Ensure access to ARD is restricted to authorized staff, officials, and agents of the parties who need it to execute their official duties which require access to the information.
3. Ensure appropriate staff training related to the privacy, security, and confidentiality of ARD and will implement training programs as deemed necessary.
4. Require certifying organizations or agencies, which require access to ARD to perform certification activities, to sign a Data Share Agreement ensuring the protection of ARD and specifying the process for transference of ARD for eligible individuals.



5. Determine the acceptable level of risk of disclosure prior to each planned release of ARD. In each specific case, the data will be evaluated for the risk of disclosure within the context that the data will be used. A safeguard strategy that is the most appropriate for that particular context will be utilized.
6. Statistically aggregate, in non-person-specific form, test responses and other information collected in the certification, credentialing, licensure, and test registration and delivery process and transfer this information to test sponsors and to independent testing centers. Such aggregated, non-person-specific information may be used for quality control, operations management, educational research, and security to enhance, develop, and/or improve certification, credentialing, licensure, testing services, and testing processes. By administering a test through NOCTI, the customer (e.g., school, agency, organization, or institution) gives consent to this non-person-specific data aggregation and the use and transmission of this aggregated statistical data.
7. Release information requested by a judicial order or legal subpoena. With respect to student ARD, the school of record must make a reasonable effort to notify the parent (or eligible student) in advance of compliance, unless the court or other issuing agency has ordered that the contents of the subpoena not be disclosed, or that the protected education records not be included.
8. Release ARD information to state and local juvenile justice authorities, if state law permits, after receiving written certification that the information will not be disclosed to any other agency, organization, or third party without the parent's permission, except as allowed in state law.

### **Data Security**

ARD is stored in electronic format on systems maintained by NOCTI in a secure data center facility located within the United States of America. The measures that NOCTI employs to protect the privacy and security of the ARD while it is stored in that manner are those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and layered password protection.

NOCTI servers are hosted by a top-ranked Network Operations Center (NOC) with a Tier 3 Data Center. The NOC has multiple redundant connections to the Internet backbone through several carriers located in different cities. Most importantly, it is designed to remain fully operational in the event of a power outage or failure of a major backbone carrier.

QuadNet™ employs RSA 2048-bit encryption. Assessment administration and related program activities occur within an encrypted web session which discourages unauthorized external access (hacking). QuadNet data is securely protected behind firewalls and Secure Socket Layer (SSL) encryption techniques to prevent hijacking and theft. User-response data has redundant fail-over systems, on-site backup, and off-site backup to guard against disaster, loss, and potential down time. NOCTI's data systems are constantly monitored electronically by technical supervisors to ensure data integrity and no interruptions to service.

**Data Destruction**

NOCTI complies with retention and disposal schedules consistent with applicable laws and state record retention and disposal schedules.

**Unauthorized Release of Data**

In the event of unauthorized release of ARD by NOCTI, its subcontractors, or assignees in violation of applicable state or federal laws, notification will be made to the affected party(s) in the most reasonable way possible.