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 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 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, 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: Darryl Agostinelli 4A54259A4AF84DF...
Printed Name:	Darryl Agostinelli
Title:	CTO
Date:	6/27/2024

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).

Name of Contractor	The New England Center for Children, Inc
Description of the purpose(s) for which Contractor will receive/access PII	So that the CABOCES team can utilize our ACE ABA Software
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII □ APPR Data
Contract Term	Contract Start Date 9/1/24 Contract End Date 8/30/25
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.

CONTRACTOR	
Signature:	DocuSigned by: Darryl Agostinelli 4A54259A4AF84DF...
Printed Name:	Darryl Agostinelli
Title:	CTO
Date:	6/27/2024

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.	NECC has adopted a Written Information Security Policy, (WISP) to: 1. protect the security and confidentiallty of PI of our employees, students, and consumers. 2. protect against any expected threats or hazards to the security or integrity of such information; and, 3. protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud. 4. detect and respond to threats of such information before affected individuals and NECC suffer substantial harm.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	NECC's WISP addresses administrative, technical, physical and operational controls at a high level and is supported by underlying policies and additional controls to protect PII and the Confidentiality, Integrity, and Availability of information assets.
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.	NECC has adopted a Security Awareness Training policy which requires all new hires, contractors, and existing staff to participate in annual security awareness training and annual data privacy training.
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.	NECC has implement a third-party Contracts policy to review supply chain risks and ensure that all contractors and vendors meet the same standards for information security as NECC has adopted. All staff and contract employees are vetted, and sign written agreements to adhere to the WISP.
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.	All information security and privacy incidents are reported, logged, and managed as part of NECC's incident response process. NECC's Crisis Response Manual addresses notification procedures as required by applicable regulatory and contractual requirements.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data reports and exports are available from within the ACE
7	Describe your secure destruction practices and how certification will be provided to the EA.	Client data is deleted directly from the database within a reasonable timeframe upon request. Email confirmation is provided stating that all data was deleted
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	NECC periodically assesses the information security program to: 1) identify reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper, or other records containing PI. 2) assess the likelihood and potential damage of these threats. 3) evaluate the sufficiency of existing NECC policies and procedures to control risks. 4) design and implement a plan that puts safeguards in place to minimize those risks; and 5) monitor the effectiveness of those safeguards. 6] assess NECC's alignment with contiols and standards described in the DocuSign Envelope ID: 0D2AD292-6CEF-4AFC-93AA-BD87D27C42B1 Page 14 of 16 NIST Cybersecurity Framework, and the NIST Privacy Framework
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)	**Asset Management (ID.AM):** 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.	NECC has inventoried physical systems, software platforms and external information systems. Information resources are prioritized, classified and appropriate toles have been established for information assets.
	Business Environment (ID.BE): 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.	NECC has identified critical dependencies and resilience requirements base upon NECC's role in the supply chain as a provider of special needs educational services.
	Governance (ID.GV): 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.	A written information security policy is in place including as ongoing information security program. All staff are aware of the policy. Executive management and board of directors receive periodic updates on he status of the information security program.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	NECC has implemented a risk management program where risks are identified, tracked and applicable actions taken based upon impact and likelihood of potential threats and vulnerabilities.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The risk management process at NECC is established with tolerances based upon NECC's role in the educational sector.
	Supply Chain Risk Management (ID.SC): 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.	NECC has implemented a third-party risk management policy and process to identify and address supply-chain risks.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** 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.	NECC manages data access by incorporating principles of least privilege determined by the information classification level. Networks are segmented, remote access is managed and controlled. Each user on NECC information systems has a unique ID and multifactor authentication is implemented and enforced.

Function	Category	Contractor Response
	Awareness and Training (PR.AT): 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.	NECC has adopted a security awareness training policy which requires all new hires, contractors and existing staff to participate in annual security awareness training and annual data privacy training.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	NECC maintains separate testing and development environments from the production ACE environment. Data in transit along with data stored on individual workstations is encrypted. NECC securely disposes or destroys data on media at the end of useful life. Disposal records are maintained.
	Information Protection Processes and Procedures (PR.IP): 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.	NECC has established a formal system development life cycle for the ACE. Backups are maintained and monitored. Incident response procedures are in place. Vulnerabilities are identified tracked, processes continually improved.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	NA
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	NECC has in place controls to protect communications and control networks. Least functionality principles are incorporated into system configurations. Audit log records are implemented.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	NECC collects event data from multiple systems and sources. Incident alert thresholds are established, and events are analyzed.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The physical environment is located in AWS and monitored by AWS. NECC has systems in place to monitor for malicious code. Vulnerability scans are performed.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NECC has defined detection roles and responsibilities. Event detection information is communicated. Detection processes are continually improved.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	NECC has established response procedures to execute during an incident.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	NECC has an established crisis response plan with defined roles and expectations for coordinating communication with internal and external stakeholders. All incidents are reported in accordance with established criteria.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Notifications from detection systems are investigated. Incidents are categorized to understand the impacts. Processes are in place to analyze and respond to disclosed vulnerabilities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Newly identified vulnerabilities are documented and either mitigated or logged as tolerated risks.

Function	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans are continually improved implementing lessons learned.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery procedures are executed to ensure restoration of systems.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned and strategies are updated.
	Communications (RC.CO): 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).	Recovery activities are communicated to internal and external stakeholders. Public relations are formally managed