

## 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:	<i>Mohsen Attarpour</i>
Printed Name:	Mohsen Attarpour
Title:	Authorized Person
Date:	4/19/2024

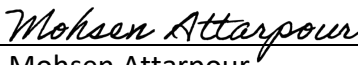
## EXHIBIT B

### 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).

<b>Name of Contractor</b>	EdClub, Inc
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Providing a subscription to EdClub products as licensed. EdClub products include web-based education tools to teach users skills such as touch typing, digital citizenship, spelling and vocabulary (among others).
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>July 1, 2024</u> Contract End Date <u>June 30, 2027</u>
<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 checked="" 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 checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input checked="" 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> <p>Data will be stored on servers located within the United States of America. Contractor will store and process data in accordance with commercial best practices, including implementing appropriate safeguards.</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>	<p>Mohsen Attarpour</p>
<b>Title:</b>	<p>Authorized Person</p>
<b>Date:</b>	<p>4/19/2024</p>

## Exhibit C

### 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 implement applicable state, federal, and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract, and applicable laws pertaining to data privacy and security including Education Law § 2-d. In addition, Contractor will comply with its data security policies, which address the NIST CSF.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	The data will be stored in the United States of America. The Contractor shall store and process confidential student records and information in accordance with commercial best practices, including implementing appropriate administrative, physical and technical safeguards.
3	Address the training received by your employees, officers 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 training to its officers, employees, or assignees who have access to PII on the federal and state law governing confidentiality of such 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 will ensure that its employees, subcontractors and third-party service providers with whom Contractor shares PII abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform their obligations in a manner consistent with the data protection and security requirements outlined therein.
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 will promptly notify EA of any Breach or unauthorized release of PII in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such Breach. Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the DPA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of the Contract, Contractor shall transfer PII to EA, in a mutually agreed upon format, provided that, EA has made such a written request within 30 days of expiration or termination of the Contract.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII will be securely destroyed within 30 days of expiration or termination of the Contract utilizing an approved method of confidential destruction, including verified erasure of magnetic media using approved methods of electronic file destruction. Thereafter, Contractor will provide

		EA with certification of such destruction upon written request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements as a "Third-Party Contractor" as outlined in 8 NYCRR Part 121 and in accordance with the EA's Policy, as well as include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement.
9	<p>Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.</p> <p>OR</p> <p>Outline how your data security and privacy program/practices materially align with the NIST CSF v 1.1. Please include details regarding how you will identify, protect, respond to, and recover from data security and privacy threats, as well as how you will manage your security controls.</p>	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

Function	Category	Contractor Response
<b>IDENTIFY (ID)</b>	<i>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.</i>	Employees are required to monitor their equipment and Contractor closely manages access to its assets according to its Minimum Access Policy.



Function	Category	Contractor Response
	<b>Business Environment (ID.BE):</b> <i>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.</i>	Contractor's Data Protection Standard and Information Security and Acceptable Use Policies explain its information security goals and are distributed to all employees.
	<b>Governance (ID.GV):</b> <i>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.</i>	Contractor publishes a comprehensive set of data security policies to all employees, which describe how it expects employees and third parties with access to its systems to behave and secure those systems.
	<b>Risk Assessment (ID.RA):</b> <i>The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</i>	Contractor's Audit Policy requires it to analyze the risks associated with processing confidential information.
	<b>Risk Management Strategy (ID.RM):</b> <i>The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</i>	Contractor's Audit Policy requires it to analyze the risks associated with processing confidential information.
	<b>Supply Chain Risk Management (ID.SC):</b> <i>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.</i>	Contractor applies the requirements of its information security policies to third parties that may have access to its systems.
<b>PROTECT (PR)</b>	<b>Identity Management, Authentication and Access Control (PR.AC):</b> <i>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.</i>	Contractor's Information Security and Acceptable Use Policy, and Minimum Access Policy, specifically identify access controls.

Function	Category	Contractor Response
	<b>Awareness and Training (PR.AT):</b> <i>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.</i>	Contractor requires employees to be trained according to its <i>Data Protection Standard</i> .
	<b>Data Security (PR.DS):</b> <i>Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</i>	Contractor's Data Protection Standard defines the minimum security standards Contractor applies to educational data.
	<b>Information Protection Processes and Procedures (PR.IP):</b> <i>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.</i>	Contractor's Minimum Access Policy sets forth procedures for, e.g., privileged account creation, terminating user access, use of authentication and encryption, etc.
	<b>Maintenance (PR.MA):</b> <i>Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</i>	Contractor's Audit Policy establishes routine review and maintenance procedures.
	<b>Protective Technology (PR.PT):</b> <i>Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</i>	Contractor's Minimum Access Policy and Password Construction and Protection Policy define how it protects relevant assets.
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> <i>Anomalous activity is detected and the potential impact of events is understood.</i>	Contractor requires monitoring for anomalous activity in its Data Breach Response Policy.
	<b>Security Continuous Monitoring (DE.CM):</b> <i>The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</i>	Contractor's Audit Policy enables continuous monitoring.



Function	Category	Contractor Response
	<b>Detection Processes (DE.DP):</b> <i>Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</i>	Contractor's Data Breach Response Policy enables defines the criteria for detection and response to anomalous events.
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> <i>Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</i>	Contractor's Data Breach Response Policy defines the procedures for responding to cybersecurity incidents and establishes a Data Breach Response Team.
	<b>Communications (RS.CO):</b> <i>Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</i>	Contractor's Data Breach Response Policy establishes communications roles.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Contractor's Data Breach Response Policy creates a procedure for responding to incidents.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Contractor's Data Breach Response Policy establishes mitigation procedures.
	<b>Improvements (RS.IM):</b> <i>Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</i>	Contractor's Data Breach Response Policy require Contractor to evaluate whether improvements to its processes are necessary.
<b>RECOVER (RC)</b>	<b>Recovery Planning (RC.RP):</b> <i>Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</i>	Contractor's Data Breach Response Policy establishes recovery procedures.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Contractor's Data Breach Response Policy requires Contractor to evaluate whether improvements to its processes are necessary.
	<b>Communications (RC.CO):</b> <i>Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems,</i>	Contractor's Data Breach Response Policy requires Contractor to communicate as necessary to prevent future incidents.

Function	Category	Contractor Response
	<i>victims, other CSIRTs, and vendors).</i>	