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-privacysecurity/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-privacysecurity/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:	Lia M. Brooks
Printed Name:	Lia M. Brooks
Title:	General Counsel
Date:	03 / 14 / 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	**Zearn**
Description of the purpose(s) for which Contractor will receive/access PII	**To provide Zearn School Account and On-Demand PD services pursuant a Zearn Master Services Agreement.**
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Contract Start Date July 1, 2024 Contract End Date June 30, 2027
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: Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	Lia M. Brooks
Printed Name:	Lia M. Brooks
Title:	General Counsel
Date:	03 / 14 / 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.	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
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor will maintain reasonable security standards appropriate to the type of data collected, which will include multiple safeguards to help protect against loss, misuse or alteration of information including encryption of data while in motion and at rest, use of two-factor authentication to access the system, regular software security updates and industry best practices for network and physical security.
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 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 Pll 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 PU to EA, in a mutually agreed upon format, provided that EA has made such a request within 15 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.
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 include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement.
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.	Zearn inventories all physical property, the software applications and access rights associated with same, Zearn advises all employees of their cybersecurity roles and responsibilities, including through annual privacy training. Cybersecurity role of third-party stakeholders is established through contract.
	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.	Priority is placed on protecting access to personally identifiable information of students, in line with our mission of serving all students to love learning math. This is communicated both internally and externally (TOU and PP) and informs all risk management decisions at the organization.
	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.	Zearn Team Policies include Confidentiality, Privacy, and Security policy and are understood and acknowledged by all employees. The General Counsel bears responsibility for educating team on cybersecurity, CTO bears responsibility for managing the settings governing data stored in Zearn's cloud platform. Zearn's third-party IT service provider provides support to Zearn on cybersecurity tools and implementation of same.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	General cybersecurity threats are identified and understood. Zearn's most vulnerable assets are identified as the student PII collected. Zearn's Incident Response Plan identifies responses to security incidents (risks related to the loss or threatened loss of data).
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk is managed through consultation and collaboration with the CEO, the General Counsel, and Executive Team. Risk tolerance is based on the awareness of Zearn's role as a guardian of student data.
	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.	The General Counsel evaluates all suppliers and third-party partners receiving customer data. The General Counsel reviews all contracts with suppliers and third-party partners to ensure Zearn's cybersecurity obligations are satisfied.

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.	Zearn manages the assets, processes, and devices that its employees have access to, both physical and logical. User identifies the credentials are provisioned or revoked based n level of access necessary to fulfill the job function. Zearn uses multi-factor authentication for employee access to student data.

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.	Zearn conducts annual privacy training for all employees. Zearn informs customers through its privacy policy, customer contracts, and ongoing user support of their roles and responsibilities; Zearn's partners are legally required to abide by security obligations no less stringent than Zearn's
	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.	Zearn encrypts personal data both at rest and in transit to protect its confidentiality, integrity and availability. Zearn's production environment is kept separate from its testing environment.
	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.	Information is protected in daily database backups. Personal data is destroyed according to internal policy and external commitments. Zearn maintains documented security policies and an incident response plan.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Zearn logs all application activity and conducts regular maintenance of information assets as necessary.
	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.	Through its third-party cloud hosting provider, Zearn uses access control and redundancy to ensure resilience of data collected and stored. The application is automatically replicated on a near real-time basis at the database layer and are backed up as part of the deployment process on secure, access controlled, and redundant Storage.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Zearn and its third-party cloud hosting provider maintain security incident management policies and procedures to detect and understand security events.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Data collected and hosted is monitored for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Physical data centers and personnel are monitored to detect potential cybersecurity incidents. Practices and software limit the risk of exposure to software viruses.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Zearn and its third-party cloud hosting provider maintain security incident management policies and procedures to detect and understand security events. Zeam's documented incident response plan identifies the roles and responsibilities of personnel.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Although Zeam has not experienced an incident requiring response, Zearn maintains a documented incident response Ian to respond to cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Zearn maintains a documented incident response plan that identifies the roles and responsibilities of personnel and includes guidelines for communicating with external stakeholders.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Zearn maintains a documented incident response plan that sets forth processes for receiving, analyzing, and responding to disclosed vulnerabilities.

	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Although Zearn has not experienced an incident requiring response, its processes include steps to contain and mitigate incidents.

Function	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	This is not applicable as Zearn has not experience an incident requiring response.
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.	This is not applicable as Zearn has not experienced an incident requiring recovery.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	This is not applicable as Zearn has not experienced an incident requiring recovery.
	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).	Zearn's incident response plan identifies the roles of personnel involved in external communications, and the executive team is informed of incident response processes.