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:	Bryan McGrath (Apr 1, 2022 12:16 CDT)
Printed Name:	Bryan McGrath Bryan McGrath
Title:	CFO CFO
Date:	Apr 1, 2022 April 1, 2022

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	eDynamic Holdings LP
Description of the purpose(s) for which Contractor will receive/access PII	Digital course access and Instructional services for eDynamic Courses
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII □ APPR Data
Contract Term	Contract Start Date July 1, 2022 Contract End Date June 30, 2025
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: eDynamic Learning utilizes Amazon AWS as a cloud solution provider. We undergo regular security reviews and follow industry best practices to ensure data safety. EDL infrastructure is being continuously monitored by Managed Deteection and Response solution (Alert logic)
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	Bryan McGrath (Apr 1, 2022 12:16 CDT)
Printed Name:	Bryan McGrath
Title:	CFO CFO
Date:	Apr 1, 2022 April 1, 2022

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN eDynamic Holdings LP

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.	eDynamic Learning utilizes Amazon AWS as a cloud solution provider. We undergo regular security reviews and follow industry best practices to ensure data safety. EDL infrastructure is being continuously monitored by Managed Detection and Response solution (Alert logic)
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	We have a wide variety of safeguards in place. Some examples of the safeguards in each category include: Operational - Contractual agreements with vendors that are regularly reviewed - Administrator Password policies - Employee training - Security Reviews - Employee Background checks
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.	EDL employees that require access to customer PII to fulfill terms of the contract receive annual privacy training. All subcontractors are under administrative obligation to provide privacy training to their employees
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.	Our subcontractors are well established educational organizations (Agilix Buzz - LMS; Genius SIS - SIS; Proximity Learning - Teachers). The subcontractors go through careful selection process to ensure their practices are acceptable to EDL. The contracts with subcontractors are carefully reviewed to ensure the best practices are outlined and enforced.
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.	We have multiple safeguards in place to help to identify breaches as quickly as possible, including our MDR services. The MDR services constantly monitors our infrastructure for attacks, unusual activity, configuration inconsistencies etc. In an unlikely event the breach becomes successful MDR service provides us with mitigation tools and recommendations.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	The data can be exported from both Buzz (LMS) and Genius SIS in a CSV format.
7	Describe your secure destruction practices and how certification will be provided to the EA.	The district has a right to request secure destruction of the district PII at any time. As the destroyed data cannot be recovered, we request a written notice from the district outlining the scope (Specific user/ group of students/ all district data). EDL will securely remove PII from its systems within 90 days of such request and provide confirmation to the district. In the case of instructional services, there are cases where eDynamic might be required to maintain certain records by law, if this is the case district will be
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	eDynamic Learning follows industry best practices to protect student data.
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.	eDynamic Learning utilizes manual and automatic asset management for EDL technical infrastructure. Development, staging and production systems are operationally and physically separated from each other and require different levels of access. Access and configurations is continuously monitored through MDR system. Business critical production applications have necessary redundancy, disaster recovery plans and continues health monitoring. Infrastructure is monitored 24x7 by both AWS management vendor (Mission Cloud) and MDR service (Alert Logic) allowing EDL to utilize top specialized resources in both fields
	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.	EDL regularly reviews systems and technology. Security and privacy planning are important parts of planning for technical projects. Roles and responsibility of stakeholders and their access to infrastructure is reviewed and only minimal possible permissions are granted.
	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.	EDL utilizes a governance system to constantly assess cybersecurity risk. Our infrastructure is constantly scanned for any best practice recommendations and the recommendations are reviewed and addressed by technology leadership. All contracts and commitments are regularly reviewed.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Cybersecurity is very important to EDL. This is why we utilize industry best to protect ourselves and our customers. Systems are constantly reviewed for security risks.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Yes, Technical team works very closely with the business side to ensure that any projects are undergo security reviews and risks are managed, addressed and prioritized.
	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.	EDL carefully reviews commitments from any subcontractors to ensure the risks are acceptable and can be managed.
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.	AWS provides industry best physical controls when it comes to infrastructure access. EDL implemented industry standard operational controls to ensure safe infrastructure access including such as two factor authentication (including hardware keys to root accounts) , SSO etc). the systems also maintain full audit logs of system access that is being constantly monitored for anomalies.

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.	We utilize best of breed security partner (Alert Logic) that gives ability to utilize highly trained security professionals. EDL tech team is constantly learning and re-evaluating its security posture based on latest industry developments.
	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.	Yes, data models and data access are consistently reviewed to ensure minimal access. The systems are constantly scanned my an MDR solution to identify any potential misconfiguration
	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.	EDL works with Mission Cloud and Alert Logic to ensure correct playbooks (processes and procedures) are in place. The Roles and responsibilities are clearly defined
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	EDL ensures that systems are properly maintained on multiple levels: Software: - Regular code maintenance - Automated dependency scans and security updates - Automated security scans OS and Managed services: - Systems are regularly patched based on AWS and Mission cloud recommendations. Changes tested on dev environments first Hardware: AWS ensures that hardware is secure and regularly maintained
	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.	Technical security solutions are automatically scanned and manually reviewed to ensure security and resilience levels are appropriate
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	MDR service (Alert Logic) detects and reports any anomalies
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	MDR service constantly monitors the system and assets and effectiveness reports are available
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	MDR services maintains and regularly tests procedures
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	MDR service maintains playbooks and records of any attempted security incident attempts
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	In case of a security breach EDL will follow industry best recommendations and guidance provided by MDR service security specialists including coordination with external resources
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Security incidents are reviewed and analyzed by MDR services and EDL staff
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	MDR service provides mitigation strategy and action to minimize the impact of the incident and to prevent it from re-occuring

Function	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Security incidents are reviewed and analyzed by MDR services and EDL staff and post-mortum is performed to incorporate any lessons learned. MDR service is able to draw lessons from other services they perform including AI analysis and applies lessons learned to all its clients
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.	Production systems have disaster recovery plans and backup policies
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	New systems and services are planned with circuit breakers and fail safes in mind. New production infrastructure is added to monitoring and has backup and recovery policies
	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).	EDL will work with internal and external stakeholders to coordinate and communicate any restoration processes.