Data Security and Privacy Information
For Imagine Learning LLC

As per section 4 of the Confidentiality and Data Security and Privacy Standards Addendum agreement, this plan must be completed by the Service Provider within 10 days of the signing of said Addendum.

1. Exclusive Purposes for Data Use
    a. The exclusive purposes for which the student data [or teacher or principal data] will be used by the service provider include

Imagine Learning provides digital K-12 curriculum and related education services including Imagine Language & Literacy.

Initial _____

2. Data Accuracy/Correction Practices
    a. Parent [student, eligible student, teacher or principal] may challenge the accuracy of the data by

In the event that a student's parent or an eligible student wishes to challenge the accuracy of student data (pertaining to the particular student) that may include records maintained,stored, transmitted, and/or generated by Contractor pursuant to the Agreement, the challenge will be processed in accordance with the procedures of the District. A teacher or principal who wishes to challenge the accuracy of data pertaining to the teacher or principal personally, which is disclosed to Contractor pursuant to the Agreement, shall do so in accordance with the procedures for challenging APPR data, as established by the District.

Initial _____

3. Subcontractor Oversight Details
    a. This contract has no subcontractors: Yes _____ No X
    b. The contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations by

Initial _____

4. Security Practices
   a. The data is stored with AWS cloud storage within the United States
   b. The security protection taken to ensure data will be protected include

Safeguards & practices: data encryption, data system monitoring, incident response plan, file transfer protocol, firewalls, secure programming practice, facility security, account protection and limited access to systems.

5. Contract Lifecycle Practices
   a. The agreement expires 6/1/2027
   b. When the agreement expires, the student data [or teacher or principal data] will be Deleted or returned in accordance with the Confidentiality Data Security and Privacy Agreement

6. Encryption Practices
   a. Data encryption is applied in accordance with Education Law 2-d 5(f)(5)
   Yes X No Initial Initial: U

7. Training Practices
   a. Annual training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student [or teacher or principal data]
   Yes X No Initial Initial: U

Imagine Learning LLC Signed by: Leslie Curtis 92AF38E8309E478...
Company Name

Leslie Curtis EVP & Chief Administrative Officer Date April 16, 2026
Print Name and Title of Contact Person

Return to:
Chris G Connors
Director of Instructional Technology, CIO, DPO
cconnors@herricks.org
516-305-8720

VENDOR DATA PRIVACY AND SECURITY PLAN

VENDOR'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. **Please fill out or reference your Data Privacy and Security Plan.**

If you already have a plan, please just reference the url here or attached document.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Imagine Learning has designated a privacy official to manage the data security and privacy regulatory and contractual obligations involving personally identifiable information and student data.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Imagine Learning maintains ISO 27001 ISMS certification. Safeguards & practices include data encryption, data system monitoring, incident response plan, file transfer protocol, firewalls, secure programming practice, facility security, account protection and limited access to systems.
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.	All employees, agents and subcontractors are required to have at least annual privacy and data security training. Employees are also encouraged to received periodic role-based privacy training throughout the year.
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.	All employees are required to sign a confidentiality agreement that protects the confidentiality of customer information. Imagine Learning enters into written agreements with its service providers who will receive PII and student data where the service provider agrees to keep all data confidential and limit use of the data to those services for which they retained.
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.	In the event that the confidentiality or integrity of personally identifiable data is compromised from an unauthorized disclosure or data breach, Imagine Learning will notify affected customers of such breach in accordance with the terms of its contract with the customer, will investigate, and will restore the integrity of its data systems as soon as possible. We will fully cooperate and assist with required notices to those individuals affected by such breach.
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 will be returned or deleted in compliance with the Data Privacy Agreement.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Imagine Learning destroys data in compliance with NIST SP 800-88 guidelines. Certification of destruction is provided to customer at the end of the services.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Imagine Learning follows industry best practices, including the ISO 27001 Information Security Management Systems cybersecurity framework and NIST cybersecurity framework, throughout the development and maintenance lifecycle of our application.
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.

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 pages if needed.

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.	Imagine Learning has policies and procedures for asset management including acceptable use, management and handling of 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.	Imagine Learning has policies and procedures for organization of information security that includes security roles and responsibilities, contact with internal and external stakeholders, and project management of activities within the company
	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.	Imagine Learning maintains ISO 27001 ISMS certification and employs security controls and policies to manage and monitor its cybersecurity risk in compliance with ISO 27001 standards.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Imagine Learning maintains policies and procedures for operations security to manage cybersecurity risks to operations, assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Imagine Learning employs risk management strategies at the organization level such as third party audits, risk assessments, disaster recovery plan, and business continuity plan.
	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.	Imagine Learning has policies and procedures for supplier management including assessment of information security requirements of suppliers, address of security in supplier agreements and change management of supplier services.

Function	Category	Contractor Response
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.	Imagine Learning has policies and procedure for access controls and physical and environmental security to limit access to systems, devices, processes and facilities.
	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.	Imagine Learning requires employees and partners to receive cybersecurity awareness education.
	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.	Imagine Learning maintains ISO 27001 ISMS certification and manages data in compliance with ISO 27001 requirements.
	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.	Imagine Learning maintains privacy and security policies in compliance with ISO 27001 ISMS requirements to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Imagine Learning performs maintenance and repairs consistent with its security policies.
	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 assessed to ensure consistency with Imagine Learning security policies, procedures and agreements.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Imagine Learning monitors activities to detect vulnerabilities and any potential impact of those vulnerabilities.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Imagine Learning monitors information systems and assets to detect vulnerabilities and any potential impact of those vulnerabilities.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes are maintained and tested to ensure awareness of suspicious events.

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Imagine Learning has an incident response plan and playbook 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).	Imagine Learning's incident response plan and playbook describe the appropriate communications with internal and external stakeholders.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Imagine Learning's incident response plan and playbook describe the appropriate communications with internal and external stakeholders.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Imagine Learning's incident response plan and playbook describe mitigation and remediation actions of a suspected or actual cybersecurity incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Imagine Learning's incident response plan and playbook describe postmortem activities to identify lessons learned and action items that need to be taken to improve services.
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.	Imagine Learning maintains recovery policies and procedures to restore systems affected by cybersecurity incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Imagine Learning's incident response plan describes postmortem activities to identify lessons learned and action items that need to be taken to improve services.
	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).	Imagine Learning's incident response plan and playbook describe the appropriate communications with internal and external stakeholders.

Vendor	
[Signature]	Signed by: Leslie Curtis 92AF58E8509E47B...
[Printed Name]	Leslie Curtis
[Title]	EVP & Chief Administrative Officer
Date:	April 16, 2026