AddendumD

PARENTS' BILL OF RIGHTS- SUPPLEMENTAL INFORMATION ADDENDUM

1. EXCLUSIVE PURPOSES FOR DATA USE: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by nter-State Studio/SLR Photograph:(the "Contractor") are limited to the purposes authorized in the contract between the Contractor and East Irondequoit Central School District (the "School District") dated July 1, 2023 - June 30, 2024 (the "Contract").

2. SUBCONTRACTOR OVERSIGHT DETAILS: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will ·disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to, those outlined in applicable State and Federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR §121).

3. CONTRACT PRACTICES: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District in excel format and/or destroyed by the Contractor as directed by the School District.

4. DATA ACCURACY/CORRECTION PRACTICES: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the School District in a Contractor's product and/or service by following the School District's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Contractor's product and/or service by following the appeal procedure in the School District's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. SECURITY PRACTICES: Confidential Data provided to Contractor by the School District will be stored in :ecure Server (See attached The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. ENCRYPTION PRACTICES: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum to Section E

SLR Photography, LLC - An independently owned and operated Inter-State Studio Franchise

(New York State Data Privacy Agreement Support Documentation)

1. Outline how you will implement applicable data security and privacy contract requirements over the life of the contract.

We conduct regularly scheduled audits of our security software and hardware configurations to verify compliance. Including but not limited to antivirus and anti-intrusion software, hardware and software firewalls, and network policies restricting access and retention of sensitive data on our internal network.

2. Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.

We employ modern security software and hardware to prevent exposure of data. We audit the settings of our software and hardware With specialists in applicable fields. We monitor and log access to PII to verify it is required and appropriate.

3. Address the training received by your employees and any subcontractors engaged in provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.

Training consists of formal education in the respective fields, monthly security training videos and tests, and dedicated time set aside to learn the proper use and execution of security software and hardware employed at Inter-State on an as-needed basis.

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.

NA

5. Specify how you will manage any data security and privacy incidents that implicate Pl! and describe any specific plans you have in place to identify breaches and/or unauthorized disclosure, and to meet your obligations to report incidents to the EA.

We log access to PII and maintain tools that allow immediate responses to the variable possible security scenarios that require unique steps to address. Any security breaches will be reported to the EA in compliance with state and federal law.

6. Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.

NA

7. Describe your secure destruction practices and how certification will be provided to the Educational Agency.

PII data is deleted from all file storage, databases and backups within the time frames defined by our internal production policies and privacy agreement.

8. Outline how your data security and privacy program/practices align with the EA's applicable policies.

per CMMC section our maturity level is (1,2,3,4,5 etc.)

9. Outline how your data security and privacy program materially align with the NIST CSF vl.1 using the Framework chart below. See the Pages Following

Exhibit C .1- NIST CSF Table

Inter-State Studio & Publishing Co. has adopted the CMMC framework for cybersecurity evaluation.

Unlike NIST SP 800-171, the CMMC model possesses five levels. The model is cumulative whereby each level consists of practices and processes as well as those specified in the lower levels. The CMMC Model includes additional cybersecurity practices in addition to the security requirements specified in NIST SP 800-171.

In addition to assessing a company's implementation of cybersecurity practices, the CMMC also assesses the company's maturity processes.

We have aligned the CMMC maturity model scale against the NIST CSF vl.1 and are reporting the CMMC categories and our related maturity level for each category on the following pages.

Additional details of the CMMC framework can be found at www.acq.osd.mil/cmmc/index.html

EXHIBIT C.1- NIST CSF TABLE

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.	C002-3, C004-1, C006-4
	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.	C033-3
	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.	C032-3
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	C031-3, C032-3, C035-3, C037-4,C040-2
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	C032-3
	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.	C032-3, C033-3
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.	C003-3, C004-1, C015-2, C038-3

	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.	C011-4, C012-2, C037-4
	Data Security (PR.OS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	C002-3, COOS-4, C014-3, C015-2, C024-1, C025-2, C038-3, C039-4
	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.	C013-2, C014-3, C023-2, C024-1, C026-2, C029-2, C037-4
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	C021-2
	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.	C002-3, C004-1, C010-4, C023-2, C038-3
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	C010-4, C013-2, C018-2
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	C002-3, C007-3, C028-2, C031-3, C032-3, C041-1
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	C017-2, C018-2, C031-3, C037-4, C041-1
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	C016-2
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	C018-2, C037-4

	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	C016-2, C018-2, C019-2, C037-4, C040-2
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	C018-2, C041-1
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	C016-2, C018-2
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.	C019-2
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	C016-2
	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).	C019-2