Supplemental Information about a Master Agreement between Mineola School District and Banzai Inc.

Mineola School District has entered into a Master Agreement with Banzai Inc. ("Banzai"), which governs the availability to the District of the following products or services:

Banzai Online Curriculum

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Addendum), the District may provide to Banzai, and Banzai may receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Banzai is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Banzai will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Banzai engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Banzai under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commenced or will commence on the date the Banzai Online Curriculum is or was first used by the District. The Master Agreement will expire as of the first date on which the Banzai receives a notice of termination from the District, or viceversa.
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Banzai will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Banzai or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Banzai will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Master Agreement is assigned to a successor Banzai (to the extent authorized by the Master Agreement), the Banzai will cooperate with the District as necessary to transition Protected Data to the successor Banzai prior to deletion.

- Neither Banzai nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Banzai and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Banzai, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Banzai by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Banzai receives will be stored on systems maintained by Banzai, or by a subcontractor under the direct control of Banzai, in a secure data center facility located within the United States. The measures that Banzai (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Banzai (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

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.	Pursuant to internally documented policies and procedures and subject to applicable law and regulation.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See the IDENTIFY and PROTECT sections of the NIST framework included below.

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.	Training and guidance provided to new employees and employees newly responsible for PII, as well as recurrent training given to all employees with access to PII.
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.	New subcontractor arrangements must be authorized by corporate officers, who are all aware of these requirements.
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.	Incidents will be managed pursuant to the requirements set forth in State Education Law 2-d, as well as under other applicable state and federal law and regulation.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Pursuant to the requirements of State Education Law 2-d after receiving a written request from the EA.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Data in production databases removed immediately; backup data securely deleted within 90 days. Certification provided upon request pursuant to applicable law.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Policies and procedures have been created that align with all applicable
		law and regulations, including those applicable to the EA.
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.

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.	NCSR Maturity Level score 7
	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.	NCSR Maturity Level score 7
	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.	NCSR Maturity Level score 7
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	NCSR Maturity Level score 6
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are	NCSR Maturity Level score 6

Function	Category	Contractor Response
	established and used to support operational risk decisions.	
	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.	NCSR Maturity Level score 7

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.	NCSR Maturity Level score 7
	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.	NCSR Maturity Level score 6
	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.	NCSR Maturity Level score 7
	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.	NCSR Maturity Level score 7
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	NCSR Maturity Level score 7
	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.	NCSR Maturity Level score 7
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	NCSR Maturity Level score 6
Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	NCSR Maturity Level score 6

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NCSR Maturity Level score 5
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	NCSR Maturity Level score 7
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	NCSR Maturity Level score 7
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	NCSR Maturity Level score 7
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	NCSR Maturity Level score 7
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	N/A (There have not been any historical incidents to which we've been required to respond.)
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.	NCSR Maturity Level score 7
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	N/A (There have not been any historical incidents from which we've been required to recover.)
	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).	NCSR Maturity Level score 6