New York Education Law Section 2-d

Data Sharing & Confidentiality Addendum

Including

Parents Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between the District and Banzai

1. Purpose

a. Lancaster Central School District (hereinafter "District") and Banzai Inc., a Delaware corporation (hereinafter "Banzai") are parties to the Banzai's Site Terms of Use and Privacy Policy (collectively, the "Master Agreement") pursuant to which Banzai may receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District.

b. If Banzai receives Protected Data, as defined below, this New York Education Law Section 2-d Data Sharing & Confidentiality Addendum (hereinafter "Addendum") shall supplement the Master Agreement, thus ensuring that the Master Agreement conforms to the requirements of Section 2-d. This Addendum consists of a provisions related to data sharing and confidentiality, the Parents Bill of Rights for Data Security and Privacy created by the District (Section 7), and the Supplemental Information about the Master Agreement between the District and Banzai (Exhibit "A") that the District is required by Section 2-d to post on its website.

c. In consideration of the mutual promises set forth in the Master Agreement, Banzai agrees that it will comply with all terms set forth in the Master Agreement and this Addendum. To the extent that any terms contained in the Master Agreement conflict with the terms of this Addendum, the terms of this Addendum will apply and be given effect.

2. Definitions

As used in this Addendum:

a. "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Banzai may receive from the District pursuant to the Master Agreement.
b. “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Banzai may receive from the District pursuant to the Master Agreement.
c. “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Banzai pursuant to the Master Agreement.
d. “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. <u>Confidentiality of Protected Data</u>

a. Banzai acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.
b. Banzai will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District’s policy on data security and privacy in the form made publicly available on the District’s website as of the date this Addendum was executed, provided that no provision of such District policy which is not expressly authorized by Section 2-d shall be binding upon Banzai.

4. <u>Data Security and Privacy Plan</u>

a. As more fully described herein, throughout the term of the Master Agreement, Banzai will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy, and security of the Protected Data it receives from the District.
b. Banzai’s Plan for protecting the District’s Protected Data includes, but is not limited to, its agreement to comply with the terms of the Parents Bill of Rights for Data Security and Privacy, a copy of which is included by reference and which has been signed by the Banzai.
c. Additional components of Banzai’s Data Security and Privacy Plan for protection of the District’s Protected Data throughout the term of the Master Agreement are as follows:
    i. Banzai will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and

this Addendum, consistent with the District's data security and privacy policy.

ii. Banzai will have specific administrative, operational, and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

iii. Banzai will comply with all obligations contained within the section set forth in Exhibit "A" ("Supplemental Information about a Master Agreement between the District and Banzai"). Banzai's obligations described within this Exhibit include, but are not limited to:

1. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Banzai by state and federal law and the Master Agreement shall apply to the subcontractor, and
2. its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

d. Banzai has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

e. Banzai will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Banzai will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Addendum.

5. <u>Notification of Breach and Unauthorized Release</u>

a. Banzai will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Banzai has discovered or been informed of the breach or unauthorized release.

b. Banzai will provide such notification to the District by contacting Michele Ziegler ("District Contact") by by email at mziegler@lancasterschools.org or by telephone at 716-686-3844.

c. Banzai will cooperate with the District and provide as much information as possible directly to District Contact or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident,

the date Banzai discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Banzai has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Banzai representatives who can assist affected individuals that may have additional questions.

d. Banzai acknowledges that upon initial notification from Banzai, the District, as the educational agency with which Banzai contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Banzai agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Banzai directly or requests more information from Banzai regarding the incident after having been initially informed of the incident by the District, Banzai will promptly inform the District Contact or his/her designee.

6. <u>Additional Statutory and Regulatory Obligations</u>

a. Banzai acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Addendum:
    i. To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA) (i.e., those who require access in order to assist Banzai in fulfilling one or more of its obligations to the District under the Master Agreement).
    ii. To not use Protected Data for any purposes other than those explicitly authorized in this Addendum and the Master Agreement.
    iii. To not disclose any Protected Data to any other party, except for authorized representatives of Banzai using the information to carry out Banzai's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:
        1. the parent or eligible student has provided prior written consent; or
        2. the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure unless such notice is expressly prohibited by the statute or court order.

iv. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

v. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

vi. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

vii. To comply with Section 2-d, Part 121, and District's policy on data security and privacy in the form made publicly available on the District's website as of the date this Addendum was executed, provided that no provision of such District policy which is not expressly authorized by Section 2-d shall be binding upon Banzai.

viii. To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

ix. To notify the District, in accordance with the provisions of Section 5 of this Addendum, of any breach of security resulting in an unauthorized release of Protected Data by Banzai or its assignees or subcontractors in violation of applicable state or federal law, the Parents Bill of Rights for Data Security and Privacy, District's policy on data security and privacy in the form made publicly available on the District's website as of the date this Addendum was executed (provided that no provision of such District policy which is not expressly authorized by Section 2-d shall be binding upon Banzai), or other binding obligations relating to data privacy and security contained in the Master Agreement and this Addendum.

x. To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

xi. To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Banzai or its subcontractors or assignees in any instance where such payment or reimbursement is required by applicable law or regulation.

7. <u>Parents Bill of Rights for Data Security and Privacy</u>

a. Banzai acknowledges and agrees that the Parents Bill of Rights for Data Security and Privacy, in the form made publicly available by the District on the District's website on the date this Addendum was executed, is hereby incorporated into this Addendum by reference.
b. Notwithstanding the foregoing, or any other language in this Addendum to the contrary, no provision of the Parents Bill of Rights for Data Security and Privacy which is not expressly authorized under Section 2-d shall be incorporated into this Addendum.

FOR BANZAI

Morgan Vandagriff, President
Dated: September 28, 2021

FOR THE DISTRICT

Michele Ziegler
Signature

Michele Ziegler / Data Protection Officer
Written Name and Title

June 2, 2022
Date

Return Countersigned Copy to Banzai Inc.
Email: privacy@teachbanzai.com
Fax: +1 (801) 228-1758
Mail: Attn: Privacy Filings
Banzai Inc.
2230 North University Parkway, Suite 14
Provo, Utah 84604

Exhibit "A"

Supplemental Information about a Master Agreement between the District and Banzai

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

Lancaster Central 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 vice-versa.
- 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