Compliance with NYS Education Law Section 2

RE: Unauthorized Release of Personally Identifiable Information Parents' Bill of Rights

Kings Park Central School District is an educational agency within the meaning of Section 2-d of the NYS Education Law. As defined in said law, the following specifications shall apply to any vendor who is a "third party contractor" who receives "personally identifiable information" regarding student, teacher or principal data.

When the Kings Park Central School District enters into contracts with an outside contractor who receives confidential student data, vendors must acknowledge that they understand and will comply with the provisions of NYS Education Law Section 2-d in all respects including but not limited to the following:

<u>Education Law Section 2-d(5)(d)</u>

Third party contractor agrees that the confidentiality of student, teacher and principal data shall be maintained in accordance with state and federal laws and the educational agency's policies on data security and privacy that protect the confidentiality of personally identifiable information.

<u>Education Law Section 2-d(5)(e)</u>

Third Party Contractor agrees that any of its officers or employees, and any officers or employees of any assignee of Third Party Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data.

<u>Education Law Section 2-d(3)(b)(1) and (c)(1)</u>

The exclusive purpose for which Third Party Contractor is being provided access to personally identifiable information is to enable Kings Park Central School District to make use of the services provided by Third Party Contractor, or by any assignee of Third Party Contractor, from Kings Park Central School District and shall not be sold or used for marketing purposes.

<u>Education Law Section 2-d(3 (c)(2)</u>

Third Party Contractor shall ensure that to the extent that it comes into possession of personally identifiable information, it will only share that personally identifiable information with additional third parties if those third parties are contractually bound to adhere to the data protection and security requirements set forth in this specification.

<u>Education Law Section 2-d(3)(c)(3)</u>

Upon expiration of an agreement with Kings Park Central School District the Third Party Contractor shall assist Kings Park Central School District in exporting all personally identifiable information pertaining to students, teachers and principals previously received from Kings Park Central School District and shall thereafter securely delete any copy of the data remaining in Third Party Contractor's possession or control. If data is to be maintained by Third Party

Contractor for federal and/or state reporting, such data shall remain in an encrypted format and stored in a secure facility located within the United States of America.

Education Law Section 2-d(3)(c)(4)

In the event that a parent, student, or eligible student or teacher or principal wishes to challenge the accuracy of student or teacher or principal data concerning that student or eligible student or teacher or principal that challenge shall be processed through the procedures provided by the Kings Park Central School District under the Family Educational Rights and Privacy Act (FERPA).

Education Law Section 2-d(3(c)(5) and (5)(e) and (5)(f)(4) and (5)(f)(S)

Student or teacher or principal data transferred to Third Party Contractor by Kings Park Central School District will be stored in electronic format on systems maintained by Third Party Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States of America. The measures that Third Party Contractor will take to protect the privacy and security of student or teacher or principal data while it is stored in that manner are associated with industry best practices including, but not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

Education Law Section 2-d(5)(f) and (6)

Third Party Contractor acknowledges that it has the following obligations with respect to any student or teacher or principal data received from the Kings Park Central School District and any failure to fulfill one of these statutory obligations shall be a breach of the agreement with Kings Park Central School District:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and FERPA including technical support;

- not use education records for any purpose other than those explicitly authorized in this Agreement;

- not disclose any personally identifiable information to any other party who is not an authorized representative of the Third Party Contractor using the information to carry out Third Party Contractor’s obligations under this Agreement, unless (1) that other party has the prior written consent of the parent or eligible student or teacher or principal, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

- maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in Its custody;

- use encryption-technology to-protect data -while.in motion or in its. custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

- notify the Kings Park Central School District of any breach of security resulting in an unauthorized release of student or teacher or principal data by the Third Party Contractor or its assignees in violation of state or federal law, the parents bill of rights for student data and security, the data privacy and security policies of the educational agency, and/or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay.

Education Law Section 2-d(6}(c)

In the case of notification to a parent, eligible student, or teacher-or principal under Education Law Section 2-d(6)(b) due to the unauthorized release of student or teacher or principal data by the Third Party Contractor or its assignee, the Third Party Contractor shall promptly reimburse the Kings Park School District for the full cost of such notification.

To ensure compliance with Education Law Section 2-d, it may be necessary to amend or modify this specification after certain regulations have been promulgated by the New York State Education Department, and the parties agree to take such additional steps as may be necessary at that time to ensure continued compliance with Education Law Section 2-d.

Kings Park Central School District Parents' Bill of Rights respects the privacy of personally identifiable information for all students and, therefore, promulgates a Parents' Bill of Rights regarding the privacy and security of student and teacher/principal data. The Parents' Bill of Rights include the following:

1. Student data cannot be sold or released for commercial purposes
2. Parents have the right to inspect and review the complete contents of their child's education record
3. State and federal law protects the confidentiality of personally identifiable information. Kings Park Central School District utilizes safeguards such as encryption, firewalls, and password protection to protect personally identifiable information.
4. A list of all student data elements collected by the state is available for public review.
5. Parents have the right to have complaints addressed about possible breaches of student data.

All vendors must sign below to verify that the above has been read and that the terms and conditions of these Documents will be adhered to.

Vendor: Thinkmap, Inc. dba Vocabulary.com

Signature: Chief Executive Officer

Purchase order. #: ______________________

Date: September 18, 2024

Kings Park Central School District

180 Lawrence Road
Kings Park, New York 11754

Parents' Bill of Rights for Data Privacy and Security

The Kings Park Central School District is committed to protecting the privacy and security of each and every student's data. Parents should be aware of the following rights they have concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by the State Education Department is available for public review at: https://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. Parents have the right to file complaints about possible breaches of student data. Parents may submit a complaint regarding a potential breach by the District to Dr. Ralph Cartisano, Deputy Superintendent, 180 Lawrence Road, Kings Park, New York 11754. The School District shall promptly acknowledge any complaints received and commence an investigation into the complaint, while taking the necessary precautions to protect personally identifiable information. The School District shall provide a response detailing its findings from the investigation no more than sixty (60) days after receipt of the complaint. Complaints pertaining to the State Education Department or one of its third party vendors may be submitted to NYSED at https://www.nysed.gov/data-privacy-security/report-improper-disclosure by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, or email to privacy@nysed.gov or by telephone at (518) 474-0937.

6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

7. If the District enters into a contract with a third party in which student, teacher, or principal data is shared with a third party, supplemental information for each such contract will be appended to this Parents' Bill of Rights.

8. Parents may access the State Education Department's Parents' Bill of Rights at: https://www.nysed.gov/common/nysed/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Acknowledged by: ____________________ Thinkmap, Inc. dba Vocabulary.com ____________________ September 18, 2024 ____________
Organization Date

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

As per the Agreement between the undersigned and the School District, this information must be completed by the Service Provider within ten (10) days of execution of the Agreement.

Name of Provider:	Thinkmap Inc.dba Vocabulary.com
Description of the purpose(s) for which Provider will receive/access PII:	Data is used for improving and providing Contractor's services to the school or on the school's behalf.
Type of PII that Provider will receive/access:	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term:	Contract Start Date: September 18, 2024 Contract End Date: September 18, 2025
Subcontractor Written Agreement Requirement:	Provider 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) ☐ Provider will not utilize subcontractors. ☒ Provider will utilize subcontractors.
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Provider shall: • Securely transfer data to the School District, or a successor provider at the School District'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 School District. If a correction to data is deemed necessary, the School District will notify Provider. Provider agrees to facilitate such corrections within 21 days of receiving the School District'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: Contractor will use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to: encryption, firewalls, and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student data of the District while in motion or in custody of Department from unauthorized disclosure.
Encryption:	Data will be encrypted while in motion and at rest.

PROVIDER	
[Signature]	Paul Mishkin
[Printed Name]	Paul Mishkin
[Title]	Chief Executive Officer
Date:	September 18, 2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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.	Contractor will implement applicable state, federal and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract and applicable laws pertaining to data privacy and security, including Education Law § 2-d.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor employs automated log collection and audit trails for production Systems. – Connections originating from untrusted network segments will be governed by firewall rules and other security safeguards that grant the minimal access required to access the intended service provided by the company. – System passwords and access keys are stored in a privileged location accessible only to security administrators, and all credentials are changed from factory default settings. – Production systems receive regular maintenance to apply security patches. – Physical access to systems requires security RFID badges and biometric authentication, and is limited to IT staff performing physical maintenance.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the	Contractor shall ensure that all its employees, officers and subcontractors who have access to PII have received or will receive training on the federal and

	Contract on the federal and state laws that govern the confidentiality of PII.	state laws governing confidentiality of such data prior to receiving access.
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.	Contractor seeks out service providers that shares their commitment to maintaining the privacy and security of Personal Data and requires their subprocessors to respect their user data to the same or greater degree as we do. Contractor has implemented a variety of physical, administrative and technological safeguards designed to preserve the integrity and security of their personal information they collect and to protect against unauthorized access to data. These include internal reviews of data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where personal data is stored. Contractor restricts access to personal information to Contractor's employees, contractors, and agents who need to know that information in order to operate, develop or improve their services.
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 School District.	Contractor maintains security incident management policies and procedures and will, to the extent permitted by law, promptly notify customers of any unauthorized disclosure of PII. Contractor maintains Security Incident Response Plan includes policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems. There are also procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and

		document security incidents and their outcomes.
6	Describe how data will be transitioned to the School District when no longer needed by you to meet your contractual obligations, if applicable.	Unless otherwise directed by a School or Parent, Contractor will delete or de-identify personal information of student and child users after a period of inactivity, after the termination or cancellation of the license subscription, or after termination of their agreement with the School, in accordance with the terms of any applicable written agreement with the School, written requests from unauthorized School administrators, and our standard data retention schedule. Authorized School administrators may contact Contractor at compliance@ixl.com to request additional information about Contractor's standard data retention schedule and available options for customizing Contractor's standard data retention schedule to meet individual School requirements.
7	Describe your secure destruction practices and how certification will be provided to the School District.	Unless otherwise directed by a School or parent, Contractor will delete or de-identify personal information of student and child users after a period of inactivity after the termination or cancellation of the license subscription, or after termination of their agreement with the School, in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and their standard data retention schedule. Authorized School administrators may contact Contractor at compliance@ixl.com to request additional information about their standard data retention schedule and available options for customizing Contractor's standard data retention schedule to meet individual School requirements.

8	Outline how your data security and privacy program/ practices align with the School District’s applicable policies.	As outlined herein, Contractor’s practices are designed and implemented with the goal of maximizing the security and privacy of all customer data. This includes limiting access to EA data to employees with a business need and encrypting all data in transit and at rest. Please inquire if more information is needed.
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 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.	Contractor have asset management controls and policies in place for physical devices and software within our organization. We have mapped organizational comms and data flows and cataloged external subprocessors. We have also categorized information systems and organizational resources in accordance with applicable company policies.
	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.	Contractor have established and communicated priorities for organizational mission and objective. We have also put in place contingency plans and disaster recovery policies to inform decisions and deliver mission critical services.
	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.	Contractor have established and communicated organizational cybersecurity policies, and coordinated and aligned roles and responsibilities with internal roles and external partners. Legal requirements and obligations regarding cybersecurity and privacy are understood and managed.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including	Contractor identify, document, and patch asset vulnerabilities on a regular schedule. We also identify, document, and remediate both internal and external threats. We identify and prioritize risk responses.

Function	Category	Contractor Response
	mission, functions, image, or reputation), organizational 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.	Contractor have established risk management processes that are agreed upon by organizational stakeholders. Contractor clearly express organizational risk tolerance, which is determined by security standards compliance and sector-specific regulations.
	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.	Contractor assess and choose third-party subprocessors, including AWS, using risk assessment processes. We use contracts with third-party partners to implement appropriate measures that manage security and risk tolerance. Our third-party partners are also routinely assessed using industry standard audits, such as SOC 2, to ensure appropriate security of information systems.
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.	Contractor manage and protect access to physical assets using RFID badges, and access is limited to IT staff performing physical maintenance. Contractor require unique user credentials and two-factor authentication to access network environments containing user data. We have policies in place for managing identity and credential lifecycles. Our production hosts run on Amazon Web Services, which is SOC 2 compliant. We limit remote access to VPN and manage ACLs by principle of least necessary privilege.
	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.	Contractor provide all personnel with IT onboarding training upon starting employment and randomly select employees for security assessment practical examination on an ongoing basis. Privileged personnel undergo additional training commensurate with their roles and responsibilities. We communicate expectations regarding additional roles and responsibilities to employees and third-party stakeholders as needed.
	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.	Contractor protect data in transit using TLS and SSH. All data stored in Vocabulary.com’s production environment is encrypted at rest using AES-256 bit encryption. Contractor use real-time replication and verify the integrity of the replica on a continuous basis. Vocabulary.com periodically creates a database clone from offline backups. Contractor use over-provisioning, redundancy, geographic distribution, and uninterruptible power supplies to ensure high availability. We also separate development and testing environments from our production environment.
	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.	Contractor create and maintain baseline configuration of systems and put system lifecycle policies in place for managing information systems. Contractor continuously conduct, maintain, and test backups of information. Contractor destroy data in accordance with policy. Contractor track changes to system configuration and put configuration change control processes in place. Contractor also implement and manage incident response and disaster recovery plans. Contractor include cybersecurity in HR practices. Contractor also have developed and implemented a vulnerability management plan.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Contractor perform and log maintenance and repair of organizational assets with approved tools. Contractor also approve, log, and perform remote maintenance of organizational assets in a manner that prevents unauthorized access.

Function	Category	Contractor Response
	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.	Contractor have implemented mechanisms to achieve resilience requirements in normal and adverse situations, including using a third-party CDN/proxy and web application firewall (WAF) to mitigate against possible DDoS attacks
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Contractor have established a baseline of network operations and expected data flows and actively monitor for events. Contractor analyze detected events to understand incidents and their impact. Contractor collect and correlate event data from multiple sources and sensors, and determine the impact of events based on that data. Contractor have also established incident alert thresholds.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Contractor monitor the network to detect potential cybersecurity events. Our physical production environment is monitored 24/7. Contractor run software internally to identify and alert us about real-time security events such as excessive failed login attempts, suspicious network traffic, etc and store event logs in a tamper-proof fashion.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Contractor have well-defined roles and responsibilities for detection and incident response, and our detection activities comply with applicable policies and requirements. Contractor seek to continually communicate and improve detection information and processes.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Contractor have documented our incident response and recovery plan and made stakeholders aware of their roles. Steps include investigation by the appropriate members of our security team, resolution via engineering (for code vulnerabilities) or IT (for OS/networking vulnerabilities), testing the fix to ensure it truly resolves the issue, and quickly applying the validated fix to production.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Contractor ensure that personnel know their roles and order of operations when response is needed. Incidents are reported and information is shared consistent with policy criteria. Contractor coordinate with stakeholders consistent with our response plans.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Contractor investigate notifications from detection systems and evaluate and categorize the impact of incidents consistent with our response plans. The goal of the investigation is to figure out where the vulnerability exists and what impact it has. Once the type of issue is identified, Contractor can move on to resolution.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Contractor contain and mitigate threats to prevent expansion of an event. We mitigate or document newly-identified vulnerabilities based on their associated risk levels.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Contractor conduct thorough postmortems for all incidents and update response strategies to account for new information learned.
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.	Contractor execute recovery plans during or after a cybersecurity incident to ensure that systems are restored. Through redundancy, geographic distribution, and offline backups, Contractor can restore data to its state up to three weeks in the past.

Function	Category	Contractor Response
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Through thorough postmortems, Contractor incorporate lessons learned and reflect new information in our recovery plans.
	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).	Contractor communicate recovery activities to internal and external stakeholders as well as executive and management teams. Contractor also comply with all state and federal requirements for notifying impacted parties.