BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Thinkmap, Inc. dba Vocabulary.com
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.
Description of the purpose(s) for which Contractor will receive/access PII	(i) providing the Service, (ii) improving and developing our Service, (iii) enforcing our rights under these Terms, and (iv) as permitted with the School's or the User's consent.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 07/01/2024 Contract End Date 06/30/2025
Subcontractor Written Agreement Requirement	Contractor 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) ○ Contractor will not utilize subcontractors. ◉ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA'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 EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA'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: Vocab employs automated log collection and audit trails for production systems. Connections originating from untrusted networks 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
Encryption	Data will be encrypted while in motion and at rest.

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 Contract on the federal and state laws that govern the confidentiality of PII.	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 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 EA.	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 EA 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 EA.	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 EA'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	Please see attached NIST CSF Table.

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

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

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Paul Mishkin
[Title]	Chief Executive Officer
Date:	05/08/2024

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.

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.	We 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.	We 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.	We 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.

Function	Category	Contractor Response
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	We 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.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	We have established risk management processes that are agreed upon by organizational stakeholders. We 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.	We 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.	We manage and protect access to physical assets using RFID badges, and access is limited to IT staff performing physical maintenance. We 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.	We 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.

Function	Category	Contractor Response
	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.	We 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. We 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. We 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.	We create and maintain baseline configuration of systems and put system lifecycle policies in place for managing information systems. We continuously conduct, maintain, and test backups of information. We destroy data in accordance with policy. We track changes to system configuration and put configuration change control processes in place. We also implement and manage incident response and disaster recovery plans. We include cybersecurity in HR practices. We 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.	We perform and log maintenance and repair of organizational assets with approved tools. We also approve, log, and perform remote maintenance of organizational assets in a manner that prevents unauthorized access.
	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.	We 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.	We have established a baseline of network operations and expected data flows and actively monitor for events. We analyze detected events to understand incidents and their impact. We collect and correlate event data from multiple sources and sensors, and determine the impact of events based on that data. We have also established incident alert thresholds.

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.	We monitor the network to detect potential cybersecurity events. Our physical production environment is monitored 24/7. We 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.	We have well-defined roles and responsibilities for detection and incident response, and our detection activities comply with applicable policies and requirements. We 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.	We 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).	We 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. We coordinate with stakeholders consistent with our response plans.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	We 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, we can move on to resolution.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	We 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.	We conduct thorough postmortems for all incidents and update response strategies to account for new information learned.

Function	Category	Contractor Response
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.	We execute recovery plans during or after a cybersecurity incident to ensure that systems are restored. Through redundancy, geographic distribution, and offline backups, we can restore data to its state up to three weeks in the past.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Through thorough postmortems, we 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).	We communicate recovery activities to internal and external stakeholders as well as executive and management teams. We also comply with all state and federal requirements for notifying impacted parties.