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

Parents(including legal guardians or personsin 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 identifierssuch 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'sidentity. 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'sidentifiable information.

4. Safeguards associated with industry standards and best practicesincluding, 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) Complaintsshould 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 regulationsif 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 practicesthat protect PII.

9. Educational agency contracts with vendorsthat receive PII will addressstatutory and regulatory data privacy and security requirements.

CONTRACTOR IXL Learning, Inc.	
[Signature]	Paul Mishkin
[Printed Name]	Paul Mishkin
[Title]	Cheif Executive Officer
Date:	03/15/2023

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 contractorsthat will receive Personally Identifiable Information (PII).

Name of Contractor	IXL Learning, Inc.
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 socialsecurity 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 b. Name c. Birthdate d. Gender e. Race f. 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	PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District, more specifically for display in reports so that teachers and district admins can see students' scoring, usage and progress and in lists so that district admins can properly organize and group students.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR PII

Contract Term	Contract Start Date: 3.15.2023 Contract End Date: 6.30.2024
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractorsto adhere to, at a minimum, materially similar data protection obligationsimposed 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, Contractorshall: • 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 protectionstaken 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: IXL 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 accessible only to IXL security administrators, and all credentials are changed from factory default settings. ● Production systems receive regular maintenance to apply security patches; and ● Physical access to systems requires security RFID badges and biometric authentication, and is limited to IT staff performing physical maintenance
Encryption	Data will be encrypted while in motion and at rest.

Western Suffolk BOCES - CONTRACTOR'SDATA 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 addressesits 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, contractorsshould 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.	IXL uses certain physical, managerial, and technical safeguards designed to preserve the integrity and security of any Personal Information and other information it maintains in connection with IXL. For example, all data is secured and protected at all times, stored on servers located in the US, and only employees with a business need to access this Personal Information are able to do so.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	All data is secured and protected at all times, stored on servers located in the US, and only employees with a business need to access this Personal Information are able to do so. Once IXL receives EA's transmission of information, it makes commercially reasonable efforts to ensure the security of its systems. IXL encrypts the transmission of all data using secure socket layer technology (SSL) or similar technologies.
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.	IXL periodically provides training to its employees regarding data security and privacy obligations with respect to such data.
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.	While IXL does not sub-contract portions of any particular contract with a customer, IXL does utilize vendors in the course of providing IXL's software. Such vendors will only be provided personally identifiable information to the extent necessary for them to provide their contracted-for services and will be subject to obligations of confidentiality and security consistent with IXL's Terms of

		Service.
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.	If IXL learns of a data security incident that compromises or appears to compromise Personal Information, then IXL will attempt to notify the users electronically so that they can take appropriate protective steps. If the subscriber is a paid School or District customer, IXL will notify the School or District electronically of any data security incident that affects the students. IXL may also post a notice on its website if a data security incident occurs.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of a School's subscriptions without renewal, IXL will delete student data and teacher or principal data in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and IXL's standard data retention schedule.
7	Describe your secure destruction practices and how certification will be provided to the EA.	When a request is received, IXL will make all efforts to delete information from its systems. IXL can provide certification upon request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	As outlined herein, IXL'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 the NIST CSF table.

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.	IXL has asset management controls and policies in place for physical devices and software within IXL's organization. IXL has mapped organizational comms and data flows and cataloged external subprocessors. IXL has 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.	IXL has established and communicated priorities for organizational mission and objectives. IXL has 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.	IXL has 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 mission, functions, image, or reputation), organizational assets, and individuals.	IXL identifies, documents, and patches asset vulnerabilities on a regular schedule. IXL also identifies, documents, and remediates both internal and external threats. Finally, IXL identifies and prioritizes 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.	IXL has established risk management processes that are agreed upon by organizational stakeholders. IXL clearly expresses 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	IXL assesses and chooses third-party subprocessors, including AWS, using risk assessment processes. IXL uses contracts with third-party partners to implement appropriate measures that manage security and risk tolerance. IXL's third-party partners are also routinely assessed

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	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.	IXL manages and protects access to physical assets using RFID badges and biometric authentication, and access is limited to IT staff performing physical maintenance. IXL requires unique user credentials and two-factor authentication to access network environments containing user data. IXL has policies in place for managing identity and credential lifecycles. IXL's production network is monitored 24x7 by a managed SOC provider. IXL limits remote access to VPN and manages 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.	IXL provides 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. IXL communicates 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.	IXL protects data in transit using TLS and SSH. All data stored in IXL's production environment is encrypted at rest. IXL takes daily backups and keeps them for 14 days. This means it can restore to any point in time for the last 2 weeks. Backups are stored in the same region as the instances as well as shipped to a geographically separate region. IXL uses over-provisioning, redundancy, geographic distribution, and uninterruptible power supplies to ensure high availability. It also separates development and testing environments from its 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.	IXL creates and maintains baseline configuration of systems and put system lifecycle policies in place for managing information systems. IXL continuously conducts, maintains, and tests backups of information. IT destroys data in accordance with policy. It tracks changes to system configuration and put configuration change control processes in place. IXL also implements and manages incident response and disaster recovery plans. It includes cybersecurity in HR practices. IXL also has 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.	IXL performs and logs maintenance and repairs of organizational assets with approved tools. IXL also approves, logs, and performs 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.	IXL has implemented mechanisms to achieve resilience requirements in normal and adverse situations, including using a third-party CDN/proxy to mitigate against possible DDoS attacks.

Function	Category	Contractor Response
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	IXL has an active contract with a managed Security Operations Center (SOC) that monitors IXL networks 24×7. Their Concierge Security Model works as an extension of IXL Security team. They provide 24×7 monitoring, detection, response, and ongoing risk management services. IXL continuously ingests/feeds critical logs such as AWS logs and system logs from servers hosted in AWS to the managed SOC provider. Upon detection of any suspicious or unusual activity, they alert the IXL Security team immediately via email. For critical/high severity alerts, they also give a phone call to the Security team members for their immediate attention.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	In addition to monitoring by the managed SOC (described above), the availability of production systems is constantly monitored by an on-call rotation of systems administrators and engineers.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	IXL has well-defined roles and responsibilities for detection and incident response, and its detection activities comply with applicable policies and requirements. IXL seeks 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.	IXL has documented its incident response and recovery plan and made stakeholders aware of their roles. Steps include investigation by the appropriate members of IXL's 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).	IXL ensures that personnel knows their roles and order of operations when response is needed. Incidents are reported and information is shared consistent with policy criteria. IXL coordinates with stakeholders consistent with its response plans.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	IXL investigates notifications from a managed SOC provider and evaluate and categorize the impact of incidents consistent with its 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, IXL can move on to resolution.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	IXL contains and mitigate threats to prevent expansion of an event. IXL mitigates or documents 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.	IXL conducts 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.	IXL executes recovery plans during or after a cybersecurity incident to ensure that systems are restored. Through redundancy, geographic distribution, and offline backups, IXL can restore data to its state up to two weeks in the past.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Through thorough postmortems, IXL incorporates lessons learned and reflect new information in the 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).	IXL communicates recovery activities to internal and external stakeholders as well as executive and management teams. IXL also complies with all state and federal requirements for notifying impacted parties.