EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Brisk Labs Corp. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Shoreham-Wading River Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information 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.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;
b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of

the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Mr. Gerard Poole
Shoreham-Wading River Central School District
250B Rt. 25A
Shoreham, NY 11786

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: **Brisk Labs Corp**

Signature: Maryel Ley

Date: **April 17, 2025**

Printed Name: **Maryel Ley**

Title: **Head of Operations**

c

1. This Bill of Rights will be included with every contract entered by the District with an outside contractor if the contractor will receive student, teacher, or principal data. This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student, teacher, or principal data, including the exclusive purpose (s) for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.

2. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

3. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, the District will notify the public via written notice, electronic notice through the District's electronic communication platform, or Telephone notification.

4. 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.

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

Contractor: **Brisk Labs Corp**

Signature: Maryel Ley **Date:** **April 17, 2025**

Printed Name: **Maryel Ley** **Title:** **Head of Operations**

EXHIBIT “B”

Contractor’s Supplemental Information

Name of Contractor	Brisk Labs Corp
Description of the purpose(s) for which Contractor will receive/access PII	Brisk Teaching utilizes student, teacher, or principal data exclusively for purposes that align with our contractual obligations and service offerings. Specifically, we use data to deliver requested services, verify user identity, and improve our platform's functionalities based on user interactions. Additionally, we employ data for analytics and research to enhance the educational value of our services, such as flagging suspicious student work and supporting learners, but do not use Student Records for marketing or advertising purposes. All data usage is executed with the overarching aim of maintaining the safety, security, and integrity of our services while complying with contractual and legal mandates.
Type of PII that Contractor will receive/access	Check all that apply: [x] Student PII [] APPR Data
Agreement Term	Agreement Start Date: April 17, 2025 Agreement End Date: June 30, 2028
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement 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 Agreement. (check applicable option): [] Contractor will not utilize subcontractors. [x] Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to District, or a successor contractor at the 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 District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the 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): [x] 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:
Encryption	Data will be encrypted while in motion and at rest.

Contractor: **Brisk Labs Corp**

Signature: Maryel Ley **Date:** **April 17, 2025**

Printed Name: **Maryel Ley** **Title:** **Head of Operations**

EXHIBIT "C"
Contractor's Data Security & Privacy Plan

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Brisk Teaching employs a multi-tiered approach to mitigate data security and privacy risks. Details below:
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	On an administrative level, access to data is restricted and a stringent disciplinary processes are in place for violations. Operationally, Brisk enforces a robust security program comprising documented policies and controls aimed at protecting confidential information against known and anticipated threats. Brisk does not permit employees to download data on devices, nor store data on removable media. Technically, we implement state-of-the- art security controls, including but not limited to encryption, firewalls, and rigorous access authorizations, bolstered by physical security measures such as encryption and role-based access controls.
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.	Brisk requires new employees with access to Confidential Information to sign a confidential agreement where they agree to comply with Data Security Policies, and to attend training on federal and state law governing Confidential Information. Brisk requires all employees with access to Confidential Information to attend a privacy training annually.
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.	Brisk will only share Student Data with subcontractors who agree to be contractually bound to, at a minimum, materially similar data protection obligations as are imposed on Brisk by applicable state and federal laws and contracts. Brisk will make available a list of all such subcontractors upon request. Brisk requires its subcontractors who have access to Student Data to properly manage and oversee their employees and assignees, including through training on federal and state privacy laws
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	Brisk Teaching has a comprehensive Incident Response plan that includes protocols for initial reporting, triage and assessment, handling and escalation, ongoing communication internally and with LEA, and post incident review. We notify LEA over email of the incident within 7 days.

	obligations to report incidents to the EA.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Brisk shall delete Student Data at any time within thirty (30) days of receipt of request by the LEA. LEA is responsible for maintaining current student classroom rosters and informing Provider to destroy Student Data which the LEA no longer needs for the purposes of this DPA and the services agreement between Provider and LEA. Upon Termination, Provider shall destroy Student Data in accordance with Provider's standard data retention policies and procedures without further notice to LEA For clarity, the duty to dispose of Student Data shall not extend to Student Data that has been De- Identified.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Brisk Teaching has implemented secure and compliant mechanisms for the disposal of student data. The disposal process is designed to remove or de- identify specific student data from our databases, logs, and other relevant storage mediums, in accordance with prevailing legal requirements and industry best practices. The specific methodology for data disposal is subject to periodic review and modification to ensure ongoing compliance and data security. Brisk Teaching will communicate to LEA that data deletion is complete.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Brisk compliance policies reflect the LEA's Data Security and Privacy Policy, in addition to relevant laws, regulations, policies and standards governing the LEA
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

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	Brisk uses administrative controls for all devices that process data.

Function	Category	Contractor Response
	objectives and the organization’s risk strategy.	
	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.	Brisk prioritizes cybersecurity efforts based on our goal to help teachers spend more time teaching, with tools that they know will protect their data and their student’s data.
	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.	Brisk maintains compliance policies, procedures, and processes to manage cybersecurity risk
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Brisk has policies in place to mitigate operational and human-based cybersecurity risks
	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Brisk maintains a risk management policy
	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.	Brisk will only share Student Data with subcontractors who agree to be contractually bound to, at a minimum, materially similar data protection obligations as are imposed on Brisk by applicable state and federal laws and contracts. Brisk will make available a list of all such subcontractors upon request. Brisk requires its subcontractors who have access to Student Data to properly manage and oversee their employees and assignees, including through training on federal and state privacy laws.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and	Brisk centralizes account management through Google SSO, and uses Google SSO to grant and revoke access to enterprise assets, and deletes or disables

Function	Category	Contractor Response
	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.	any dormant accounts after a period of 45 days of inactivity.
	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.	Brisk requires new employees with access to Confidential Information to sign a confidential agreement where they agree to comply with Data Security Policies, and to attend training on federal and state law governing Confidential Information. Brisk requires all employees with access to Confidential Information to attend a privacy training annually.
	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.	Brisk implements and maintains a risk-based information security program that uses encryption and maintains administrative, technical, and physical safeguards.
	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.	On an administrative level, access to data is restricted and a stringent disciplinary processes are in place for violations. Operationally, Brisk enforces a robust security program comprising documented policies and controls aimed at protecting confidential information against known and anticipated threats. Brisk does not permit employees to download data on devices, nor store data on removable media.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Brisk employees use up-to-date machines and software
	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.	Technically, we implement state-of-the-art security controls, including but not limited to encryption, firewalls, and rigorous access authorizations, bolstered by physical security measures such as encryption and role-based access controls.

Function	Category	Contractor Response
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Brisk monitors its services for and detects anomalous activity
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Brisk implements a cloud security posture management service that performs security checks, aggregates alerts, and enables automated remediation.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Brisk implements a cloud security posture management service that performs security checks, aggregates alerts, and enables automated remediation.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Brisk Teaching has a comprehensive Incident Response plan that includes protocols for initial reporting, triage and assessment, handling and escalation, ongoing communication internally and with LEA, and post incident review.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Brisk Teaching has a comprehensive Incident Response plan that includes protocols for initial reporting, triage and assessment, handling and escalation, ongoing communication internally and with LEA, and post incident review.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Brisk Teaching has a comprehensive Incident Response plan that includes protocols for initial reporting, triage and assessment, handling and escalation, ongoing communication internally and with LEA, and post incident review.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	All incidents include an Incident Review, where we create plans to prevent the incident from happening again
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	All incidents include an Incident Review, where we create plans to prevent the incident from happening again
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are	Recovery processes and procedures are part of Brisk's incident response plan

Function	Category	Contractor Response
	executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Brisk updates recovery processes and procedures as part of Incident Review
	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).	Internal and external communications protocols are outlined in Brisk's incident review.