E DUCATION 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 ABCYA (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 Cleveland Hill Union Free School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

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 and/or Participants' 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 Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), if applicable.

"**Protected Data**" includes any information rendered confidential by 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 and/or a Participant. 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 and/or its Participants as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District and/or its Participants 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.

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 and/or its Participants 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 and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that aligns with the NIST Cybersecurity Framework and includes the following elements:

1. A provision incorporating the requirements of the District's Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Contractor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Contractor's policy on data security and privacy.

3. An outline of the measures taken by Contractor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how Contractor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how Contractor will ensure that any subcontractors, persons or entities with which Contractor will share Protected Data, if any, will abide by the requirements of Contractor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

Contractor shall ensure any the subcontractors, persons or entities that Contractor will share Protected Data with, if any, will abide by contractual obligations with respect to Protected Data set forth herein.

Contractor hereby acknowledges that it is aware of and agrees to abide by the District's Bill of Rights, attached. A copy of this signed document must be made a part of Contractor's data security and privacy plan.

SIGNATURE: _____

TITLE: Chief Executive Officer

DATE: 12/5/2023

D ATA PRIVACY AND SECURITY PLAN

1. Attached hereto is a copy of Contractor's Data and Privacy Plan.

2. Attached hereto is a copy of the District's Bill of Rights signed by Contractor.

CLEVELAND HILL UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. This document contains a plain English summary of such rights.

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 educational records maintained by the Cleveland Hill Union Free School District.

3. State and Federal Laws protect the confidentiality of personally identifiable student information, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by New York State is available for review at the following website:

   h ttp://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

   The list may also be made available by writing to:

   Office of Information & Reporting Services
   New York State Education Department
   Room 863 EBA,
   89 Washington Avenue
   Albany, NY 12234

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Cleveland Hill Union Free School District
   Attn: John Marino, Technology Coordinator
   Cleveland Hill Union Free School District
   Cheektowaga, New York 14225
   Email: jmarino@clevehill.org
   Phone: 716-836-7200 (extension 8575)

   OR

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234

Email: CPO@mail.nysed.gov

6. Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

    a. The exclusive purposes for which the student data or teacher or principal data will be used.

    b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party 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 and principal data upon expiration of the agreement.

    d. If and how a parent, student, a student over eighteen years of age, 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, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

    a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

    b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

    c. Not use educational records for any other purpose than those explicitly authorized in the contract;

    d. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

g. Notify the Cleveland Hill Union Free School District of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;

i. Provide a signed copy of this Bill of Rights to the Cleveland Hill Union Free School thereby acknowledging that they aware of and agree to abide by this Bill of Rights

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Third-Party Acknowledgement

As a third-party contractor, I acknowledge that our contract with the Cleveland Hill Union Free District necessitates the receipt of student data and as such, requires adherence with NY State Education Law 2-d and the District's Parents' Data Bill of Rights for Data Privacy and Security. In this regard, we acknowledge our responsibility to adhere to the noted elements of the document, and have instituted processes to abide by same.

Paul Mishkin	Chief Executive Officer	ABCya.com., LLC		12/5/2023
Name	Position	Company	Signature	Date

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.	ABCya.com (ABCya) has asset management controls and policies in place for physical devices and software within our organization. ABCya has mapped organizational comms and data flows and cataloged external subprocessors. ABCya 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.	ABCya has established and communicated priorities for the organizational mission and objective. ABCya has also implemented 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.	ABCya 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.	ABCya identifies, documents, and patches asset vulnerabilities on a regular schedule. ABCya also identifies, documents, and remediates both internal and external threats. ABCya 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.	ABCya has established risk management processes that are agreed upon by organizational stakeholders. ABCya clearly expresses organizational risk tolerance, 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.	ABCya assesses and chooses third-party subprocessors, including Stripe, AWS, Sendgrid, and GSuite, using risk assessment processes. ABCya uses 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 the 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.	ABCya manages and protects access to physical assets using RFID badges and biometric authentication, and access is limited to IT staff performing physical maintenance. ABCya requires unique user credentials and two-factor authentication to access network environments containing user data. ABCya has policies in place for managing identity and credential lifecycles. Our production network hosts utilize intrusion detection system software, and our production data center, hosted by AWS, is SOC 2 compliant. ABCya limits remote access to VPN and manages ACLs by the 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.	ABCya provides all personnel with IT onboarding training upon starting employment and randomly selects employees for security assessment practical examination on an ongoing basis. Privileged personnel undergoes additional training commensurate with their roles and responsibilities. ABCya 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.	ABCya protects data in transit using TLS and SSH. All data stored in ABCya's production environment is encrypted at rest using AES-256 bit encryption. Our database has automated backups enabled, and ABCya has separate development, staging, and production environments.
	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.	ABCya creates and maintains baseline configuration of systems and puts system lifecycle policies in place for managing information systems. ABCya continuously conducts, maintains, and tests backups of information. ABCya destroys data in accordance with policy. ABCya tracks changes to system configuration and puts configuration change control processes in place. ABCya also implements and manages incident response and disaster recovery plans. ABCya includes cybersecurity in HR practices. ABCya 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.	ABCya performs and logs maintenance and repair of organizational assets with approved tools. ABCya 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.	ABCya 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
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	ABCya has established a baseline of network operations and expected data flows and actively monitors for events. ABCya analyzes detected events to understand incidents and their impact. ABCya collects and correlates event data from multiple sources and sensors and determines the impact of events based on that data. ABCya has 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.	ABCya has some alarm monitors with our AWS route 53 DNS management and Slack, and our payment processor will alert us of any unusual behavior. ABCya has implemented rate limiting on all requests that come into our API along with Google reCaptcha verification to proceed with more secure API requests. Our front end is hosted/distributed via Netlify, which also offers various levels of protection and status monitoring.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	ABCya has well-defined roles and responsibilities for detection and incident response, and our detection activities comply with applicable policies and requirements. ABCya 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.	ABCya has documented our incident response and recovery plan and made stakeholders aware of their roles. Steps include an 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).	ABCya ensures that personnel knows their roles and order of operations when a response is needed. Incidents are reported and information is shared consistent with policy criteria. ABCya coordinates with stakeholders consistent with our response plans.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	ABCya investigates notifications from detection systems and evaluates and categorizes 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, ABCya can move on to resolution..
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	ABCya contains and mitigates threats to prevent expansion of an event. ABCya 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.	ABCya conducts thorough postmortems for all incidents and updates 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.	ABCya executes recovery plans during or after a cybersecurity incident to ensure that systems are restored. Through redundancy, geographic distribution, and offline backups, ABCya can restore data to its state up to one week in the past.

	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Through thorough postmortems, ABCya incorporates lessons learned and reflects 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).	ABCya communicates recovery activities to internal and external stakeholders as well as executive and management teams. ABCya also complies with all state and federal requirements for notifying impacted parties.