NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Liverpool Central School District

and

ABCya!

This Data Privacy Agreement ("DPA") is by and between the Liverpool Central School District("EA"), an Educational Agency, and ABCya! ("Contractor"), collectively, the "Parties". This Agreement modifies the ABCya Terms of Use, available at www.abcya.com/terms/.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency 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.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 9/21/2020 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("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); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et

seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.
Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**
State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**
Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit. Contractor shall be required to comply with the obligations of this section only to the extent that such auditing or inspection activities are mandated by applicable federal or state law.

6. **Contractor's Employees and Subcontractors.**

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training.**

Contactor shall ensure that all its employees 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.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. **Data Return and Destruction of Data.**

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction. Certain residual data may persist in backups that are not used or accessed in the ordinary course of business, and which are overwritten according to the standard retention schedule for backup datasets. To the extent that such backups are restored, the de-identification process (es) shall be re-executed so that such residual data in the restored backup is deleted or destroyed. Contractor may use and retain de-identified data both during and after the term of the Agreement.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect

identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Daniel Farsaci

Title: Director of Technology

Address: 190 Blackberry Road

City, State, Zip: Liverpool, NY 13090

Email:] dfarsaci@liverpool.k12.ny.us

13. **Cooperation with Investigations.**

Contractor agrees that it will cooperate with the EA 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' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

   In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

   This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
BY: *[Signature]*	BY: *[Signature]*
[Printed Name]	**Paul Mishkin**
[Title]	**CEO**
Date:	Date: 1/21/21

EXHIBIT A - 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.

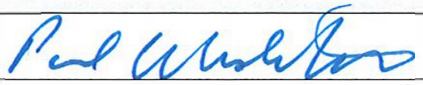
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: dfarsaci@liverpool.k12.ny.us. (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]	CEO

Date:	

EXHIBIT B

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	**ABCya.com, LLC**
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.** **Please see the ABCya Terms of Use at www.abcya.com/terms/**
Type of PII that Contractor will receive/access	Check all that apply: X☐ Student PII ☐ APPR Data
Contract Term	Contract Start Date _1/21/2021_____ Contract End Date __1/21/2022_____
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.

	X☐ 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 X☐ Other: PII will be stored in the United States. Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/ Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	**Paul Mishkin**
[Title]	**CEO**

Date:	

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Please see the ABCya Privacy Policy at https://www.abcya.com/privacy/
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	ABCya 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 ABCya 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.

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.	ABCya periodically provides such training to such individuals. Please see the ABCya Terms of Use at www.abyca.com/terms/ for more information
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.	Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/
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.	ABCya takes reasonable steps to protect the confidentiality and security of Personal Information collected from Platform users. We also take reasonable steps to release Children's Personal Information, if any, only to service providers and third parties who are capable of and have agreed to maintain the confidentiality and security of that information.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please see the attached IXL Security Policies and Procedures and ABCya's Privacy Policy, found at www.abcya.com/privacy/
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	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.**
	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 Stripe, AWS, Sendgrid, and GSuite, 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 biometric authentication, 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 network hosts utilize intrusion detection system software, and our production data center, hosted by AWS, 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.
	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 ABCya's production environment is encrypted at rest using AES-256 bit encryption. Our database has automated backups enabled, and we have 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.	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 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.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	We have some alarm monitors with our AWS route 53 DNS management and Slack, and our payment processor will alert us of any unusual behavior. We have 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.	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.
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 one week 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.