

EXHIBIT A - Bill of Rights for Data Security and Privacy
Cheektowaga-Sloan Union Free School District

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Cheektowaga-Sloan Union Free School Client is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the Client informs the school community of the following:

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 education records.
3. State and federal laws protect the confidentiality of personally identifiable 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 public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed.

Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.


CONTRACTOR	
[Signature]	
[Printed Name]	Joy Deep Nath
[Title]	Co-founder, StudyPad Inc. dba SplashLearn
Date:	1/19/2022

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	StudyPad Inc. dba SpalshLearn
Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input checked="" type="checkbox"/> APPR Data
Contract Term	Contract Start Date 1/19/2022 Contract End Date 6/30/2025
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> 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	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input checked="" type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Click or tap here to enter text.</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Click or tap here to enter text.</p> <p>Splash Math has documented a data breach response plan, which includes notification to affected consumers within a reasonable time frame. We are committed to honoring state regulations pertaining to data breaches that usually define the maximum time period for communication, mode, and content of communication as well as assigning liability</p>
Encryption	Data will be encrypted while in motion and at rest.

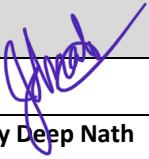
CONTRACTOR	
[Signature]	
[Printed Name]	Joy Deep Nath
[Title]	Co-founder, StudyPad Inc. dba SplashLearn
Date:	1/19/2022

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.	All communication with our application takes place over an encrypted secure connection (HTTPS / SFTP). The persistent data stores used by Splash Math are encrypted at rest.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	SplashLearn uses third party analytics services, to which only anonymized information is shared. There are other third-party applications such as Emailing Services, CRM Services, Customer Support, and Ticketing where PII like email addresses are shared. We do not share personal information of students/teachers/administrators/ parents with any third-party application
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.	SplashLearn has an internal data security team that conducts periodic trainings for team members who have access to PII.
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.	SplashLearn employs various safeguards, including monitors and alerts, periodic internal audits and assessments, external assessment once a year.
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.	SplashLearn has documented a data breach response plan, which includes notification to affected consumers within a reasonable time frame. We are committed to honoring state

		regulations pertaining to data breaches that usually define the maximum time period for communication, mode, and content of communication as well as assigning liability.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	The data is anonymised in our system
7	Describe your secure destruction practices and how certification will be provided to the EA.	Once the data is anonymised in our system we don't provide any certificates but can give an acknowledgement to the POC via email
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please refer to our privacy policy which answers these questions. https://www.splashmath.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.	SplashLearn manages data, personnel, devices, systems, and facilities consistent with organizational objectives and the organization's risk strategy including asset classification based on risk, criticality, and business value, inventory management, and establishing workforce cybersecurity roles and responsibilities.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this	SplashLearn understands and prioritizes its mission, objectives, stakeholders, and activities to inform cybersecurity roles, responsibilities, and risk management decisions.

Function	Category	Contractor Response
	information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	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.	SplashLearn understands and establishes the policies, procedures, and processes necessary to manage and monitor regulatory, legal, risk, environmental, and operational requirements and informs its management of 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.	SplashLearn understands the cybersecurity risk to organizational operations, organizational assets, and individuals including threat identification and risk determination,
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	SplashLearn establishes priorities, constraints, risk tolerances, and assumptions used to support operational risk decisions.
	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.	SplashLearn establishes priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risk, including identification and assessment of third party partners of information systems, components, and services.
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.	SplashLearn manages and limits access to physical and logical assets and associated facilities to authorized users, processes, and devices consistent with the assessed risk of unauthorized activities and transactions including identity and credential management.
	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.	SplashLearn provides periodic role-based training to individuals with access to PII, including, but not limited to training on the state and federal laws that protect personally identifiable information, and how individuals can comply with such laws. Contractor will provide training to subcontractors or ensure that its subcontractors provide annual training.
	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.	SplashLearn manages information and records (data) consistent with its risk strategy to protect the confidentiality, integrity, and availability of information, including encryption of data-at-rest and data-in-transit when required by agreement or law.

Function	Category	Contractor Response
	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.	SplashLearn maintains security policies, processes, and procedures used to manage protection of information systems and assets, including vulnerability management, incident response and business continuity.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	SplashLearn performs maintenance and repairs of information system components consistent with policies and procedures.
	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.	SplashLearn manages technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	SplashLearn detects anomalous activity and understands the potential impact of events.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	SplashLearn monitors information systems and associated assets to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	SplashLearn maintains and tests detection processes and procedures to ensure awareness of anomalous events.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	SplashLearn executes and maintains response processes and procedures to ensure response to detected cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	SplashLearn coordinates response activities with internal and external stakeholders including establishing criteria for the consistent reporting of potential incidents.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	SplashLearn r conducts an analysis to ensure effective response and support recovery activities including establishing processes to receive, analyze, and respond to identified vulnerabilities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	SplashLearn performs activities to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from	SplashLearn improves organizational response activities by incorporating lessons learned from current and previous detection/response activities.

Function	Category	Contractor Response
	current and previous detection/response activities.	
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.	SplashLearn executes and maintains recovery processes and procedures 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.	SplashLearn improves recovery planning and processes by incorporating lessons learned into future activities.
	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).	SplashLearn coordinates restoration activities with internal and external parties.