PROVIDER'S DATA PRIVACY AND SECURITY PLAN

Provider 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 Nassau BOCES' website, Provider should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

Name of Provider: Front Porch Inc. dba, Get More Math
Address: P.O. Box 5045 Sonora, CA 95370
Email/Phone: privacy@getmoremath.com/209-288-5585

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Get More Math uses security measures that are designed to protect Personal Information from accidental loss, disclosure, misuse, and destruction. These include administrative, physical and technical safeguards such as information security policies and procedures, employee privacy and security awareness training, cloud data centers that are ISO and NIST certified, and Amazon Web Services which is NIST 800-171 Certified . We restrict access to student personal information to our employees and contractors who have a direct "need to know" in order to operate and improve our services. We review our security policies, practices and procedures regularly and have security team focused on the continual improvement these processes.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Get More Math has a comprehensive information security program, based on Governance, Risk, and Compliance. We use security measures that are designed to protect Personal Information from accidental loss, disclosure, misuse, and destruction. These include administrative, physical and technical safeguards such as information security policies and procedures, employee privacy and security awareness training, using cloud data centers that are ISO and NIST certified, and Amazon Web Services which is NIST 800-171 Certified. We restrict access to student personal information to our employees and contractors who have a direct "need to know" in order to operate and improve our services. We review our security policies, practices and procedures regularly and have security team focused on the continual improvement of these processes. Get More Math has taken the Student Privacy Pledge & are currently a member of the The Student Data Privacy Consortium (SDPC).
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.	Get More Math has an ongoing Security Awareness training program that includes email phishing campaigns, specific security and privacy awareness modules that include educational content such as FERPA, COPPA, and other modules. Each employee and contractor are required to participate in ongoing training and to complete specific modules when they are hired and on an annual basis.
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.	Employees & Contractors consent by reading the Employee Information & Security Policy at the time of hire and at each annual evaluation by signing an Employee Policy Review and Acknowledgement form after reviewing the document. The document gives rights to Get More Math/Front Porch Inc. to monitor and/or audit an employees or contractors use. The policy also states that failure to comply could result in disciplinary actions. We have not and currently do not plan on contractors having access to PII.
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 Nassau BOCES.	If a possible data breach is reported to or suspected by any Get More Math employee, they will immediately send an email with "Possible Data Breach" in the subject line to security@getmoremath.com. The email should have who, what, when, where, why and how the suspected data breach occurred and sent as soon as possible. Please follow up with a call to the Director of Information Security at 209-288-5500. The Director of Information Security and the Security Team will coordinate an investigation of the suspected data breach immediately. Upon confirmation of a data breach, the Security Team will coordinate with the appropriate department to take necessary steps to contain the data breach. The Security Team will record the time of the confirmed data breach and the time of the containment and or resolution, along with who, what, when, where, how and why information on the events that led to the data breach and to the containment or resolution of the data breach. Information on any and all action taken to correct or contain the data breach will recorded in an incident report. The Director of Information Security or a Security Team member will notify the appropriate contact at the local education agency or school district and deliver the "Notification of Data Breach" that was created using the incident report.
6	Describe how data will be transitioned to Nassau BOCES when no longer needed by you to meet your contractual obligations, if applicable.	The EA will submit a request of the data they would like to have transitioned to them at the the time of the termination of the contract. Get More Math will work to get them the data in a timely manner. Once data is transitioned to EA, then Get More Math will proceed with the destruction of information practices.
7	Describe your secure destruction practices and how certification will be provided to Nassau BOCES.	After accounts are closed, we may retain that user's Personal Information if we believe that retention is reasonably necessary to comply with our legal obligations, meet regulatory requirements, meet contractual requirements with the school, resolve disputes between users, prevent fraud and abuse, enforce the Get More Math Privacy Policy and our Terms and Conditions, or to otherwise provide the Services, including but not limited to any support-related reporting and trend analysis. For active school accounts Get More Math will not delete any data on teachers or students unless requested by the school, except in the case of student accounts that have been inactive for over a year.

8	Outline how your data security and privacy program/practices align with Nassau BOCES' applicable policies.	See Template Below.
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.

NIST CSF TABLE

Providers 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, Provider 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.	Data includes student and teacher PII, employee personal information, and contractors personal information. Devices and systems include personal computers, mobile devices, software, and cloud infrastructure. · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.13.2.1, A.11.2.6, A.8.2.1, A.6.1.1
	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.	The mission of Get More Math is to provide an educational experience for students to become more efficient at mathematics. More specifically provide services to teachers and students to have access to assigned work, play available games, keep track of progress & performance, create & maintain student and teacher accounts, and prevent fraudulent use of services. · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, A.11.2.2, A.11.2.3, A.12.1.3, A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1

Function	Category	Contractor Response
	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.	Employees & Contractors consent by reading the Employee Information & Security Policy at the time of hire and at each annual evaluation by signing an Employee Policy Review and Acknowledgement form after reviewing the document. The document gives rights to Get More Math/Front Porch Inc. to monitor and/or audit an employees or contractors use. The policy also states that failure to comply could result in disciplinary actions. · ISO/IEC 27001:2013 A.5.1.1, A.6.1.1, A.7.2.1, A.18.1
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets, and individuals.	Perform Risk Assessment Overview and document these risk. This information can also be used as a way of evaluating risk and to show customers that a custom report is generated by the security team. · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3, A.6.1.4
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.	KnowB4 Compliance Manager is used to track this information. This information is used to make decisions about what risk's need mitigated while performing our goals.
	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.	Not Applicable to Get More Math and the service they p
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.	The physical and logical assests have limited access based on need and role and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.2.2, A.13.1.1, A.13.2.1, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.13.1.3

Function	Category	Contractor Response
	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.	Get More Math has an ongoing Security Awareness training program that includes email phishing campaigns, specific security and privacy awareness modules that include educational content such as FERPA, COPPA, and other modules. Each employee and contractor are required to participate in ongoing training and to complete specific modules when they are hired and on an annual basis. · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
	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.	Get More Math has an access control policy for data in place. This is limited to those only with an operational need. · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.4, A.14.1.2, A.14.1.3, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.12.1.4
	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.	Get More Math has an Information Security Policy in place. This policy aligns with ISO27001. · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2., A.16.1.6, A.16.1.1, A.17.1.1, A.7.1.1, A.7.3.1, A.8.1.4, A.12.6.1, A.18.2.2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance is performed regularly and is consistent with policies and procedures. · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.15.1.1, A.15.2.1
	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.	Get More Math has several protective security systems in place. · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Get More Math has employees that monitor system logs and metrics on a daily basis. · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4

Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Get More Math has automated systems in place to alert operations teams of negative events. · ISO/IEC 27001:2013 A.12.4.1, A.12.2.1, A.12.5.1, A.14.2.7, A.15.2.1, A.12.6.1
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Automated systems are reviewed periodically.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	If a possible breach is reported to or suspected by any Get More Math employee, they will immediately send an email with “Possible Breach” in the subject line to security@getmoremath.com. The email should have who, what, when, where, why and how the suspected breach occurred and sent as soon as possible. Please follow up with a call to the Director of Information Security at 209-288-5500. The Director of Information Security and the Security Team will coordinate an investigation of the suspected data breach immediately. Upon confirmation of a breach, the Security Team will coordinate with the appropriate department to take necessary steps to contain the breach. The Security Team will record the time of the confirmed breach and the time of the containment and or resolution, along with who, what, when, where, how and why information on the events that led to the breach and to the containment or resolution of the breach. Information on any and all action taken to correct or contain the breach will recorded in an incident report. The Director of Information Security or a Security Team member will notify the appropriate contact at the local education agency or school district and deliver the “Notification of Breach” that was created using the incident report. · ISO/IEC 27001:2013 A.16.1.5
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (*e.g.*, external support from law enforcement agencies).	Get More Math has an Incident Report Procedure that is followed. · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1, A.6.1.3, A.16.1.2
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Get More Math has an Incident Report Procedure that is followed. · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects and resolve the incident.	NIST 800-6300A Risk mitigation is followed. · ISO/IEC 27001:2013 A.16.1.5, A.12.2.1, A.12.6.1
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Get More Math holds meetings after each activity to de
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.	Get More Math has a Back Up and Restoration Procedure that is followed. · CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

Function	Category	Contractor Response
🟩	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	Get More Math implements the next steps from the lessons learned that were discussed in the meetings following an activity. · COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	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).	A task force would work to communicate the information to the needed parties to handle the effects of the attack and respond to them. · COBIT 5 EDM03.02 · COBIT 5 MEA03.02 · NIST SP 800-53 Rev. 4 CP-2, IR-4