EDUCATION LAW 2-d RIDER

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

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

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

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

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

Notwithstanding the foregoing, the parties agree that aggregate, anonymized or de-identified data derived from the Protected Data (i) is not Protected Data nor personally identifiable information; and (ii) may be used by Contractor for its data analytics, marketing, research or other commercial purposes in compliance with applicable federal and New York state laws, rules and regulations.

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

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's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

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

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Great Minds PBC

BY: Richesh Ruchir
Signed: 5/1/2023

DATED:

Richesh Ruchir, Chief Technology Officer

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Data Security Policy

Domain:	Technology
Information Classification:	N/A
Policy Owner:	Collin Hachwi, IT Director
Executive Sponsor:	Richesh Ruchir, CTO
Policy Approval Date:	
Policy Effective Date:	1-JAN-2021

1.0 PURPOSE

At Great Minds PBC (hereinafter "Great Minds"), data protection is a critical business requirement and various federal and state laws impose data security and privacy obligations on Great Minds, including, but not limited to COPPA and FERPA. As a result, it is important that all data received from schools, school districts or departments of education which we contract with to provide Great Minds products and services ("Customers" or "Educational Agencies") are reasonably and appropriately managed to maintain data integrity, accessibility, and when required, confidentiality to protect against accidental or unauthorized access, modification, disclosure, and destruction.

2.0 SCOPE

This policy applies to all Great Minds employees, contractors, consultants, temporary employees, sub processors, guests, and any other users, including all personnel affiliated with third parties who have access to Great Minds information technology resources or customer data.
This policy also applies to all data on computing, mobile devices, networking, and information resources procured through, operated, or contracted by Great Minds and any computing device connecting to or utilizing Great Minds information resources.

3.0 DEFINITIONS

"Student Data" means Personally Identifiable Information (as defined below) from Student (as defined below) records that the Company receives or has access to from Educational Agencies (as defined below) with which it contracts to provide Great Minds products and services for the educational needs of its Students or which it acquires from a Student using the Great Minds products or services. Student de-identified data, aggregate data and data elements that are not deemed Personally Identifiable Information under applicable federal and state law are specifically excluded from the definition of Student Data.

"**Personally Identifiable Information**" as applied to Student Data, means PII as defined in 34 C.F.R. §99.3 implementing the Family Educational Rights and Privacy Act ("FERPA"), at 20 U.S.C. 1232g. 2.

"**Teacher or Principal Data**" means personally identifiable information from the records of a Customer relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under applicable state or federal law. Teacher or Principal de-identified data, aggregate data and data elements that are not deemed Personally Identifiable Information under applicable federal and state law are specifically excluded from the definition of Teacher or Student Data.

"**Customer Protected Data**" means collectively, Student Data and Teacher or Principal Data. Student Teacher and Student de-identified data, aggregate data and data elements that are not deemed Personally Identifiable Information under applicable federal and state law are specifically excluded from the definition of Customer Protected Data.

"**Third Party Contractor**" means any person or entity, other than an Educational Agency, that receives Student Data and/or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing Great Minds products or services, including, but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.

"Parent" means a parent, legal guardian, or person in parental relation to a Student (as defined below).

"Student" means any person attending or seeking to enroll in an Educational Agency.

"Eligible Student" means a student eighteen years or older.

"NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

"**Unauthorized Disclosure**" or "**Unauthorized Release**" means any disclosure or release of Student Data or Teacher or Principal Data to a third party outside of the Educational

Agency prohibited by federal or state statute or regulation, any lawful contract or written agreement, or that is not in response to a lawful order of a court or tribunal or other lawful order.

4.0 POLICY STATEMENT

It shall be the responsibility of the IT Operations and Security Team to provide adequate protection and confidentiality of all corporate data, PII, and proprietary software systems, whether held centrally on local storage media, or remotely, to ensure the continued availability and integrity of the data and programs to all authorized members of staff, and to protect the security and confidentiality of Educational Agency information.

1. **Data Protection**
   Great Minds uses industry best practices encryption methods and products to protect Data both during transmissions and at rest in compliance with the NIST Cybersecurity Framework:
   - **a. Encryption in Transit**
     All data transferred over public networks is encrypted via Secure Sockets Layer (SSL) and HTTPS/Transport Layer Security (TLS).
   - **b. Encryption at Rest**
     Data at rest is encrypted using at least AES-256 or higher levels of encryption. Great Minds shall not make copies of Customer Protected Data except as reasonably necessary to provide the Service and for backup purposes.

2. **Data Review, Correction or Deletion**
   Upon termination or expiration of the Customer agreement for Great Minds products and services pursuant to which Great Minds is processing Customer Protected Data , Great Minds shall, upon Customer's or Parent's request and subject to the limitations described in the Customer's data privacy agreement, transfer all Customer data to Customer , delete the Customer data from all Great Minds systems within the period specified in the Customer agreement or applicable state law and will certify such destruction upon Customer request.

   In the event that a Parent, Eligible Student, Teacher or Principal wishes to review, modify or delete their or their Student's data shared with or acquired by the Company, the request shall be processed through the procedures provided by the applicable Educational Agency for amendment of education records under FERPA or applicable state law.

3. **Access Control**

   Great Minds follows the "Principle of Least Privilege", with the intent of reducing access and only allowing employees access to the tools, systems, and data they need to perform their job in the context of Great Minds' mission to provide high-quality educational resources to public schools. Access to production systems are role-based, centralized, auditable, and regularly reviewed. Great Minds will take reasonable steps to ensure that no person shall be appointed by Great Minds to process Customer Protected Data unless that person:

   a) is competent and qualified to perform the specific tasks assigned by Great Minds;
   b) has been authorized by Great Minds;
   c) has undergone Great Minds' training with respect to FERPA, COPPA and state student privacy laws; and
   d) has been instructed by Great Minds in the requirements relevant to the performance of the obligations of Great Minds, in particular the limited purpose of the data processing.

4. **Asset Management**

   All Great Minds assets are tracked and managed within a central repository. All corporate laptops are full-disk encrypted and wiped per industry standards when decommissioned.

   All infrastructure equipment housing Customer Protected Data resides within certified third-party data centers within AWS. AWS currently uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. All Student Data and Teacher or Principal Data from Educational Agencies in the United States resides on servers located within the United States.

5. **Passwords**

   Great Minds requires industry best practices around password requirements and storage. Furthermore, we require Single Sign On ("SSO") with multi-factor authentication requirements internally, as well as an option for our Customers who wish to use SSO.

6. **Change Management**

   All changes to Great Minds software follow our change management process and require testing and approval prior to release to production in order to avoid any accidental disclosure or release of Customer Protected Data.

7. **Business Continuity and Disaster Recovery**

   Great Minds will ensure that the systems where Customer Protected Data is stored have a disaster recovery plan that addresses geographic availability, multiple site availability,

and replication of critical systems and data. Great Minds will ensure that its third-party data center has adequate Disaster Recovery plans in place and that they are tested annually. All networking components, load balancers, web servers and application servers that are part of the Great Minds platform are configured in a redundant configuration. All Customer Data is automatically backed up daily. Great Minds performs regular recovery testing.

8. Incident Management and Breach Notification

Great Minds maintains security incident management policies and procedures. Great Minds will promptly and in any case within the period specified in Customer Data Protection Agreements and by applicable state law notify the Customer in the event Great Minds becomes aware of (I) an actual or reasonably suspected Unauthorized Disclosure or Unauthorized Release of Customer Protected Data, (ii) the Educational Agencies affected, (iii) the number of Students, Parents or Teachers affected, and (iv) the names of the Students, Parents and Teachers affected.

In the event an Educational Agency is required under applicable federal or state law to notify affected Student(s), Parent(s), Teacher(a) and/or Principal(s) of an Unauthorized Disclosure or Unauthorized Release of Student Data and/or Teacher or Principal Data by the Company or its assignees or Third-Party Contractors, the Company may be responsible for costs of such notification, subject to the terms of the Customer's Data Protection Agreement.

Great Minds may also be responsible if there are required security breach notification obligations to state governmental authorities.

9. Risk Management

Our approach to enterprise risk management at Great Minds has multiple layers, designed to focus on how we address risk as part of ongoing business operations throughout the year, not just as a point-in-time exercise on an annual basis. Great Minds maintains enterprise and cybersecurity risk assessment procedures, including annual risk assessments.

10. Security Training

All new Great Minds employees and Third-Party Contractors attend security training during the on-boarding process. Additionally, all existing employees and third-Party Contractors are required to take annual information security awareness training as well as training on elements of FERPA, COPPA and applicable state privacy laws. Training is tracked and monitored for compliance.

11. Third-Party Audit and Compliance

Great Minds is currently in the process of preparing for a SOC 2 Type 2 audit, which will be performed by an external third-party. Once completed, a copy of the report will be available subject to execution of a non-disclosure agreement ("NDA" upon Customer request**.**

12. **Threat and Vulnerability Management**

In compliance with industry best practices, Great Minds uses several sources and tools for identifying, tracking, responding to, and fixing vulnerabilities. We subscribe to relevant security mailing lists for our operating systems, software, datastores, load balancer, web frameworks, and languages.

a. **Vulnerability Management and Penetration Testing**
We perform regular and continuous scans of our systems to identify vulnerabilities. Great Minds performs annual penetration tests performed by a third-party. Reports are available under NDA upon Customer request.

b. Patch Management
Patches and upgrades are deployed system wide via our configuration management software, after review and testing. Patches are applied based on the severity level of the vulnerability according to our patch management guidelines.

13. **General Controls**

Great Minds will implement, or be responsible for its Third-Party Contractor's implementation of, measures designed to protect Covered Protected Information including:

a. deny unauthorized person's access to data-processing equipment used for processing Customer Protected Data (equipment access control);
b. prevent the unauthorized reading, copying, modification or removal of data media containing Customer Protected Data (data media control);
c. prevent unauthorized inspection, modification or deletion of stored Customer Protected Data (storage control);
d. prevent the use of automated data-processing systems by unauthorized persons using data communication equipment used to process Customer Protected Data (user control);
e. limit access to Customer Protected Data by persons authorized to use an automated data-processing system to the scope and duration of their access authorization (data access control);
f. enable verification of the individuals to whom Customer Protected Data has been transmitted or made available using data communication equipment (communication control);

g. enable verification of which individuals input Customer Protected Data into automated data-processing systems and when (input control);
h. prevent the unauthorized reading, copying, modification or deletion of Customer Protected Data during transfers of that data or during transportation of data media (transport control);
i. enable restoration of installed systems used to process Customer Protected Data in case of interruption (recovery);
j. ensure that the functions of the system used to process Customer Protected Data perform, that the appearance of faults in the functions is reported (reliability) and prevent stored Customer Protected Data from corruption by means of a malfunctioning of the system (integrity).

14. Logging and Monitoring

Great Minds shall ensure that all Great Minds systems used to store Customer Protected Data log information to our centralized log and monitoring tool so that access to such data can be audited.

15. Intrusion Detection

Great Minds or an authorized third party, will monitor our systems for unauthorized intrusions using network-based, log-based, heuristic, and signature-based intrusion detection mechanisms.

16. Physical Security

Great Mind's third-party data centers have an access system that controls access to the data center. This system permits only authorized personnel to have access to secure areas. The facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, biometric access screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

17. Human Resource Security

a. Employee Handbook

- All Great Minds employees must read and agree to the company policies, including Code of Business Conduct outlined in the Great Minds Employee Handbook.

b. Acceptable Use Policy (AUP)

Our Acceptable Use Policy outlines requirements around:

- Hardware, Software, Mobile Device, e-mail, and Network Use;
- Social Media; and
- Data Classification, Handling, and Ownership

c. **Non-Disclosure Agreement (NDA)**
All employees and Third-Party Contractors must sign an NDAor similar obligations of confidentiality prior to employment. And must abide by the provisions of this Policy.

5.0 POLICY REVIEW

The Policy Owner is responsible for reviewing the Policy at least annually to confirm that it remains current, relevant and is effective in meeting the stated business objectives.

6.0 RELEVANT POLICIES AND PROCEDURES

- Information Technology Security Incident Response Procedures
- Information Technology Security Incident Response and Notification Policy
- Data Retention and Privacy Policy
- Acceptable Use Policy

Record of Signing

For Great Minds PBC
Name Richesh Ruchir
Title Chief Technology Officer

Signed on 2023-05-01 17:27:53 GMT

Secured by Concord™
DocumentID: YTdhZjk5NjMtNz
SigningID: ZDk3YTRmNjQtM2
Signing date: 5/1/2023
IP Address: 100.36.52.68
Email: richesh.ruchir@greatminds.org