ATTACHMENT C
DATA SECURITY AND PRIVACY PLAN

Branching Minds, Inc., having offices at 157 Columbus Avenue (hereinafter the "Company") and Southern Westchester Board of Cooperative Educational Services, having offices at 17 Berkley Drive, Rye Brook, New York 10573 (hereinafter "Southern Westchester BOCES") hereby agree to make this Data Security and Privacy Plan part of their Agreement, dated May 14, 2020, for products and services and it shall be Attachment C to that Agreement (hereinafter the "Agreement").

1 Definitions: Terms used in this Data and Security Privacy Plan (hereinafter the "Plan") shall have the same meanings as those found in Education Law Section 2-d(1) and the Regulations of the Commissioner of Education at Section 121.1 of Title 8 of the New York Codes, Rules and Regulations (8 NYCRR § 121.1), unless more broadly defined herein.

2 Company is a "Third Party Contractor" as that term is defined in the Education Law Section 2-d(1) and the Regulations of the Commissioner of Education at Section 121.1 of Title 8 of the New York Codes, Rules and Regulations (8 NYCRR § 121.1).

3 Outline how the Company will implement all state, federal and local data security and privacy requirements over the term of the Agreement in a manner that is consistent with the data security and privacy policies of Southern Westchester BOCES and the component school districts and the school districts within the service area of the Lower Hudson Regional Information Center that purchase Company's products and/or services pursuant to the Agreement ("Customers"):

We know that privacy is tremendously important to our partners. A summary of our security practices is included in our privacy policy, accessible at: http://www.branchingminds.com/privacy-policy.

These practices include the following:

At Company, we are serious about our data safeguarding responsibilities. We have implemented several security measures to protect PII from unauthorized disclosure.	
NIST CSF	Company is regularly aligned with the NIST Cybersecurity Framework

Alignment	
Data Encryption	Data is encrypted in transit and at rest.
File Transfer Protocol	Data is securely transferred to Branching minds using File Transfer Protocol (FTP) over secure (SSL/TLS) cryptographic protocol.
Firewalls	Anti-virus software and firewalls are installed and configured to scan our system. The firewall is periodically updated and configured so users cannot disable the scans.
Data Storage Provider	We store all of our data and host Company's systems at secure off-site facilities managed by industry-leading Amazon Web Services (AWS) at their secured data centers in the United States. These data centers are housed in nondescript facilities and physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely. All access to the information within Company stored on these servers is encrypted. User passwords are also encrypted and all data stored with AWS on their computers is secured behind a firewall.
Security audits	Company conducts internal security audits and code reviews.
Secure programming practices	Company software developers are aware of secure programming practices and strive to avoid introducing errors in our application (like those identified by OWASP and SANS) that could lead to security breaches.
Account protection	Each user of Company is required to create an account with a unique account name and password.
Facility Security	Company is located inside the continental United States. Physical access is protected by electronic access devices, with monitored security and fire/smoke alarm systems.
Data retention and	All PII provided to Company will be destroyed upon termination of our relationship with the school or district, or when it is no longer needed for the

management	purpose for which it was provided.
Staff Training and Background Checks	All employees undergo regular training on security best practices. All employees and contractors with access to PII or who work onsite undergo background checks.
Third Party Vendor Monitoring	All Company vendors are monitored by Company on an ongoing basis to ensure they utilize industry-standard privacy precautions.
Password Protection	All Company employees utilize an encrypted password storage system to safeguard sensitive login information.

In addition to the security practices above, Company's system is also designed to give administrators flexibility to limit staff access to student information. After the initial onboarding process, teacher users have access to students listed on their class rosters, while manager users have access to all students at their school (or district). Teacher users can then either request to access to students from, or be assigned students by a manager user. In addition, teacher users and manager users can be assigned to multiple schools within a district.

Restricted access to individually identifiable student and personnel data based on defined system roles to meet all FERPA requirements.
Company's system is designed to give administrators flexibility to limit staff access to student information and to ensure that student and personnel data is protected in accordance with all FERPA requirements.

After the initial onboarding process, teacher users have access to students listed on their class rosters in Active Directory, while manager users have access to all students at their school (or district). Teacher users can then either request, or be assigned students who they do not initially have access too. In addition, teacher users and manager users can be assigned to multiple schools within a district.

Company's system utilizes a permission system to ensure that student data is accessible to teacher users that are working with that student. Conversely, administrators are able to see all data at the campus and district level, depending on their access level.

Restricted access to individually identifiable student progress to staff members involved in educational support planning for the student and defined administrators.
By default, Company's system restricts teacher user access to only those students who appear on their official school roster (as provided Company via student information system). Manager users (typically those coordinating the RTI/MTSS process, such as campus and district administrators, counselors and specialists such as school or district psychologists), who are defined explicitly by the district during implementation planning and onboarding, have access to all students at their school. Teacher users can then either request, or be assigned students who they do not initially have access too, by manager users. Both types of users may be assigned to multiple schools by system's manager users, as necessary.

4 Specify the administrative, operational and technical safeguards and practices the Company has in place to protect personally identifiable information that it receives, maintains, stores, transmits or generates pursuant to the Agreement:

This is addressed in item 3._____

_____

_____

_____

_____

_____

_____

5 The Company represents and warrants that the information contained in the Supplemental Information portion of the Parents' Bill of Rights for Data Privacy and Security of Southern Westchester BOCES with respect to the Agreement, as stated in Schedule C-1 to this Plan, is accurate.

6 Describe how officers and employees of the Company and its subcontractors and assignees who will have access to the student, teacher or principal data of Southern Westchester BOCES or of the Customers have received or will receive training on the federal and state laws governing the confidentiality of such data prior to receiving access to the data:

All employees undergo training on security best practices and federal and state laws governing the confidentiality of student, teacher or principal data.

_____

_____

_____

_____

_____

7 Will the Company utilize sub-contractors in the performance of the Agreement? (check one)

☐ Yes

X No

If Yes, how will the Company manage the sub-contractors to ensure personally identifiable data and information is protected?

_____

_____

_____

_____

_____

8 How will the Company manage data privacy and security incidents that involve personally identifiable data or information, including but not limited to (a) what actions are taken to check for and identify data breaches and unauthorized disclosures of personally identifiable information or data and (b) how Southern Westchester BOCES and the Customers will be notified promptly of any data breaches and unauthorized disclosures of personally identifiable data or information?

a. Company will utilize data loss prevention tools to monitor for data breaches or unauthorized disclosure of personally identifiable information or data at Company's endpoints. Company also utilizes universal endpoint management tools to monitor the integrity of all endpoints, ensure that the latest software and security patches have been applied, enforce the use of strong passwords, rapidly wipe endpoint devices in the event they are lost or stolen, and other protective measures.

b. In the event of a Security Breach, the Company shall promptly institute the following:

- Provide the name and contact information for an employee of the Company who shall serve as the primary security contact and shall be available to assist you twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach;

- Notify Southern Westchester BOCES and the Customer, but no later than twenty-four (24) hours after the Company becomes aware of it.

9 Upon the expiration or termination of the Agreement, if requested by Southern Westchester BOCES, Company will assist Southern Westchester BOCES in exporting all student, teacher or principal data previously received from Southern Westchester BOCES or generated by the

Company pursuant to the Agreement. In addition, all information and data of Southern Westchester BOCES remaining in Company's possession will be (check those that are applicable and fill in required information):

X Returned to Southern Westchester BOCES by August 31, 2021in the following format(s): CSV flat files, PDF_____

X Securely deleted and/or destroyed by August 31, 2021 in the following manner

- Data is destroyed using National Institute of Standards and Technology (NIST) clear method sanitization that protects against non-invasive data recovery techniques.
- Sensitive data will not be disposed of using methods (e.g.; file deletion, disk formatting, and one-way encryption) that leaves the majority of data intact and vulnerable to being retrieved.

_____.

_____

☐ Other – explain _____

_____

_____

X If student data or teacher or principal data is to be maintained by Company for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Company in a secure data facility located within the United States.

☐ Upon the expiration or termination of the Agreement, if requested by Customers, Company will assist Customers in exporting all student, teacher or principal data previously received from Customers or generated by the Company pursuant to the Agreement. In addition, all information and data of Customers remaining in Company's possession will be:

X Returned to Southern Westchester BOCES by August 31, 2021in the following format(s): CSV flat files, PDF_____

X Securely deleted and/or destroyed by August 31, 2021 in the following manner

- Data is destroyed using National Institute of Standards and Technology (NIST) clear method sanitization that protects against non-invasive data recovery techniques.
- Sensitive data will not be disposed of using methods (e.g.; file deletion, disk formatting, and one-way encryption) that leaves the majority of data intact and vulnerable to being retrieved.

_____.

_____

☐ Other – explain _____

_____

X If student data or teacher or principal data is to be maintained by Company for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Company in a secure data facility located within the United States.

BRANCHING MINDS, INC.

157 Columbus Avenue
5th Floor
New York, NY 10023

Signature: David Magier

Printed: David Magier

Title: Chief Operating Officer

SOUTHERN WESTCHESTER BOARD OF COOPERATIVE EDUCATION SERVICES
c/o Lower Hudson Regional Information Services
44 Executive Boulevard
Elmsford, New York 10523

Signature: Stephen Tibbetts

Printed: Stephen Tibbetts

Title: Asst. Superintendent for Business & Admin. Services

SCHEDULE C-1

[Signed copy of Southern Westchester BOCES Parent Bill of Rights]

Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Southern Westchester Board of Cooperative Educational Services ("Southern Westchester BOCES") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

(1) New York Stated Education law Section 2-d (Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assure the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In additions, the Southern Westchester BOCES will, upon request of parents, legal guardians or eligible students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll. An eligible student is a student who has reached 18 years of age or attends a postsecondary institution.

(2) A student's personally identifiable information cannot be sold or released for any commercial purposes;

(3) Personally, identifiable information includes, but is not limited to:

i. The student's name;

ii. The name of the student's parent or other family members;

iii. The address of the student or student's family;

iv. A personal identifier, such as the student's social security number, student number, or biometric record;

v. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

vi. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

vii. Information requested by a person who the Southern Westchester BOCES reasonably believes knows the identity of the student to whom the education record relates.

(4) In accordance with FERPA, Section 2-d and Southern Westchester BOCES Policy No. 6320, Student Records: Access and Challenge, parents and legal guardians have the right to inspect and review the complete contents of their child's education record.

(5) Southern Westchester BOCES has the following safeguards in place: Encryption, firewalls and password protection, which must be in place when data is stored or transferred.

(6) New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review at the following links or can be obtained by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234:

http://www.p12.nysed.gov/irs/data_reporting.html
http://data.nysed.gov/
http://www.p12.nysed.gov/irs/sirs/documentation/nyssisguide.pdf

(7) Eligible students, parents and legal guardians have the right to have complaints about possible breaches of student data addressed. Any such complaint should be submitted, in writing, to the Data Protection Officer of Southern Westchester BOCES at dpo@swboces.org or at 450 Mamaroneck Avenue, Harrison, New Yorkk 10528. Parents can direct any complaints regarding possible breaches via the electronic form on the Southern Westchester BOCES home page, under Resources, and Student Privacy. The complaint form can also be found by going to https://bit.ly/swbdatabreach. Alternatively, a written complaint may also be submitted to the Chief Privacy Officer of the New York State Education Department using the form available at http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure or writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

Supplemental Information for Agreement with Branching Minds, Inc. (hereinafter "Company")

(1) The personally identifiable student data or teacher or principal data (collectively, "the Data") received by Company will be used exclusively for the following purpose(s):

- ☐ To provide contracted educational services. For example, Company collects information about a student's English language proficiency in order to determine the best learning interventions to recommend for that student.
- ☐ To conduct statistical research. Any data used for this purpose is de-identified (made anonymous by removing all personally identifiable information). This research helps us evaluate the effectiveness of the Platform and improve our product.

(2) The Company will ensure that all subcontractors and other authorized persons or entities to whom Data will be disclosed will abide by all applicable data protection and security requirements, including those mandated by New York State and federal laws and regulations, by the following means:

All Company vendors are monitored by Company on an ongoing basis to ensure they utilize data protection and security measures, including those mandated by New York State and federal laws and regulations. As part of our monitoring process, Company may require vendors to respond to a questionnaire or will otherwise research the vendor's practices based on publicly available information.

(3) The Agreement with Company commenced on July 1, 2021. The initial term ends on June 30, 2021; however, the term is automatically renewed for 12 month periods unless Company or Southern Westchester BOCES provide notice of non-renewal at least thirty days prior to the expiration of the applicable term. Upon the expiration or termination of the Agreement, all Data will be (check all that apply and fill in required information):

X Returned to Southern Westchester BOCES by August 31, 2021in the following format(s): CSV flat files,
PDF_____

X Securely deleted and/or destroyed by August 31, 2021 in the following manner

- Data is destroyed using National Institute of Standards and Technology (NIST) clear method sanitization that protects against non-invasive data recovery techniques.
- Sensitive data will not be disposed of using methods (e.g.; file deletion, disk formatting, and one-way encryption) that leaves the majority of data intact and vulnerable to being retrieved.

_____.

_____

☐ Other – explain _____

_____

_____

X If student data or teacher or principal data is to be maintained by Company for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Company in a secure data facility located within the United States.

(4) In the event that a student's parent or guardian or an eligible student seeks to challenge the accuracy of student data pertaining to the particular student, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures of Southern Westchester BOCES. In the event that a teacher or principal seeks to challenge the accuracy of teacher or principal data pertaining to the particular teacher or principal, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures Southern Westchester BOCES has established for challenging annual professional performance review ("APPR") data.

(5) Describe where the Data will be stored (in a manner that will protect data security) and the security protections that will be taken by Company to ensure the Data will be protected and data security and privacy risks mitigated:

Company stores all of data and hosts system at secure off-site facilities managed by industry-leading Amazon Web Services (AWS) at their secured data centers in the United States. These data centers are housed in nondescript facilities and physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely. All access to the information within Company stored on these servers is encrypted. User passwords are also encrypted and all data stored with AWS on their computers is secured behind a firewall._____ _____

_____

_____

_____

(6) Describe how the Data will be protected using encryption while in motion and at rest:

Data is encrypted in transit using PKI and is encrypted at rest using AES-256_____

_____

Company Name: Branching Minds, Inc.

Authorized Signature: David Magier

Authorized Signer's Name & Title: David Magier, Chief Operating Officer

Date: 5/1/20