

## **EXHIBIT D**

### **DATA SHARING AND CONFIDENTIALITY AGREEMENT**

INCLUDING  
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY  
AND  
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

#### **1. Purpose**

- (a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

#### **2. Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.
- (d) “Participating Educational Agency” means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor’s Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor’s Product pursuant to the MLSA to support its own educational programs or operations.

### 3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES’s policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor’s continued compliance with Section 2-d.

### 4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES’ Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor’s Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES’ data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor’s policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: **MIND Education's posted Privacy Policy for ST Math and all of MIND's websites may be found at [www.stmath.com/privacy-policy](http://www.stmath.com/privacy-policy) and is detailed below:**

MIND Research Institute ("MIND", "we", "us", "our") has created this privacy policy to demonstrate our commitment to the privacy of our partners / customers, online visitors, and users of our websites, mobile applications, and other software. The following statement explains our information-gathering and dissemination practices for the websites at mindresearch.org and stmath.com, as well as such other websites and mobile applications as may be operated by MIND (the "Site(s)"), including our ST Math® software products that may be accessed by students or teachers via such sites and applications (the "Software"), and the versions of our Software that are licensed by parents or legal guardians for homeschool use. This Privacy Policy is part of and incorporated into the Terms of Use of the Site and the Homeschooling EULA (as defined below). This policy may change periodically, but any changes will be posted on the Site. Please refer to MIND Research Institute Privacy Policy periodically when visiting, browsing, or using any portion of the Site. Your continued use of any portion of the Site after the effective date of any changes to the Privacy Policy constitutes your agreement to the changed terms. **IF YOU DO NOT AGREE TO FUTURE CHANGES TO THIS PRIVACY POLICY, YOU MUST STOP USING THE SERVICES AFTER THE EFFECTIVE DATE OF SUCH CHANGES.**

#### Who are the Users of the Sites?

Certain of our Sites host our ST Math® instructional Software, which has been developed for use by students from pre-kindergarten through high school ("Student(s)"), for the improvement of math-related skills and achievement. Students are provided access to our Software and Sites through their schools and school districts (collectively, "Local Educational Agencies" or "LEAs"), who utilize these services to assess their Students' progress and supplement their mathematics curriculum. Homeschooled Students may also access versions of our Software that are licensed by their parent or legal guardian for homeschool use, per the terms of our end user license agreement for such Software ("Homeschooling EULA"). "Users" of our Sites include these Students; authorized representatives of the LEAs, including the Students' teachers ("LEA Representative(s)"); parents / legal guardians of the Students ("Parent(s)"); and other visitors to our websites and mobile applications ("Visitor(s)").

#### What Student information does MIND Research Institute receive via LEAs?

We are engaged by LEAs to provide the services described herein to them and to their Student Users. To utilize the Software, LEA devices are activated, and students obtain user names and passwords in order to utilize the software. We receive one or more of the following types of information regarding each Student User either directly from their LEA, or through the Student's use of the Software via their school / LEA ("Student Records"): the Student's legal name; name of the Student's teacher; name of the course in which the Software is used, if applicable; the Student's grade in school; the school and school district; the Student's user name and password (in text or and/or pictorial form); date-of-birth; the Student's identifier assigned by the LEA. Student Records may also include additional Student information owned, controlled by the LEA

and provided to us in connection with research studies that we conduct at the applicable LEA's discretion, including the Student's ethnicity; free/reduced lunch status; English-learner status; special-needs status; test scores / performance, separate from the Software. To the extent that we receive any of the foregoing as Student Records provided by or on behalf of an LEA, such Student Records shall remain owned and controlled by the LEA. We will not use or share any personal or sensitive information contained in Student Records for commercial purposes unrelated to the operation of the Sites or the services provided to the applicable LEA, Students, parents, or teachers, or for any other purposes other than those expressly described herein, the Terms of Use, or the Homeschooling EULA. We do not knowingly collect any personally identifying information regarding the Parents or other family members through the LEAs, except to the extent that such family members are themselves Students whose Student Records are provided via a LEA hereunder; for the avoidance of doubt, we may collect personally identifying information that is voluntarily provided by Visitors to our Sites, as described elsewhere under this Privacy Policy.

What Student information does MIND Research Institute collect itself from the Sites and Software?

We may collect or generate certain information automatically from the Student's use of the Sites, including login and logout timestamps. We may also collect and generate additional information about students through their use of the Software ("Student Performance Data"), including measurements / assessments of Student's progress against the ST Math® curriculum (for example, Learning Objectives encountered, passes, fails) as well as applicable educational standards; ST Math® quiz scores; and information derived and reports generated from the foregoing information and the Students' use of the Software, for utilization by the Students, their parents / legal guardians, teachers, and the LEAs.

How does MIND Research Institute use Student Records?

We may use Student Records for the following purposes:

- To monitor and generate Student Performance Data, and provide students, parents, and/or the students' teachers or LEAs, with Student Performance Data;
- To operate our software and Sites, including personalizing / customizing content for the applicable Students, reviewing / analyzing Site performance; authenticating Students; maintaining the Sites; and protecting the security or integrity of the Sites.

We may also use aggregated or de-identified information about Students, from which we have removed personally identifying information, for educational research, analysis, and similar purposes.

For the avoidance of doubt, we will not utilize any personally identifiable information in Student Records for the purposes of targeted advertising.

We do not utilize Student Records for any purposes other than those set forth in this Privacy Policy, the Terms of Use, or, if applicable, the Homeschooling EULA.

What Other Personal Information does MIND Research Institute collect from its Users?

Additional information gathered by the MIND Research Institute via the Sites falls into the following categories: (1) information voluntarily supplied by Visitors through optional online forms completed by such Visitors of our Sites when requesting additional information about MIND Research Institute or its products or services, or through Communications (as defined below) with MIND Research Institute; (2) information automatically obtained from the use of User names and password to access the restricted portion(s) of the Sites (the "Restricted Pages") to do things such as view online demonstrations or presentations about MIND Research Institute or its products or services, including, by way of example, pages visited and

time stamps; and (3) tracking information gathered as Visitors navigate through our websites or mobile applications.

MIND Research Institute may provide Users with opportunities to contact us via e-mail, conventional mail, or other methods, with questions or comments you may have about our Site, products and services, personnel, employment opportunities, or any other matter of interest to you ("Communications"). These Communications may also include e-mail attachments or any materials that you would like to send us. Any Communications and materials attached thereto that you provide to MIND Research Institute will be treated as non-confidential and non-proprietary. Please see our Terms of Use for additional information regarding how such Communications are treated.

In visiting or using our Site and in transmitting Communications with us, we may request and collect the following types of personally identifiable information from Visitors including: legal name; business name (if applicable); e-mail address; or user name and password). MIND Research Institute may also ask for additional personal information from Visitors at various times such as when we run a promotion or contest or conduct a survey, as described in such promotion or contest or elsewhere on the Site. The personally identifying information we collect from Visitors helps us offer Visitors more personalized features, respond to Visitor requests, provide you with information that is of most interest to you, improve our products and services, and, to the extent that you consent to such communications, send you promotions and events offered by MIND Research Institute.

#### Does MIND Research Institute track my IP address?

When you visit the Site, our servers automatically collect information about your Internet address (which is a number that lets computers attached to the Internet know where to send you data). Your Internet address does not identify you personally. We log your Internet address to deliver our web pages to you upon request, help diagnose problems with our servers, administer our Site in order to constantly improve its quality and the services we offer you, and identify and authenticate you and your licensed content and preferences as you navigate the Site. We may also use your Internet address to gather broad demographic information. We may also track and analyze non-identifying and aggregate usage and volume statistical information from our Visitors and other Users and provide such information to third parties.

#### How does MIND Research Institute use information collected from me?

The MIND Research Institute researches our customers' and Visitors' demographics based upon information provided by them or, their LEAs (if applicable), gathered from their Communications or password, or contained in our server log files or surveys. We do this to better understand and serve our customers and other Visitors. This research is compiled and analyzed on an aggregated basis.

#### How does MIND Research Institute share information?

MIND Research Institute does not provide, sell, trade, or rent personally identifiable information. We may disclose or share personally identifying information as follows:

##### **To our service providers.**

We may share personally identifying information collected through the Site or otherwise in our possession with companies and organizations that perform services on our behalf, for example, companies that provide data management or other support services to us (such as data storage and Web hosting services), subject to confidentiality and security obligations.

##### **For compliance with law.**

We may disclose personally identifying information to comply with applicable law, including requests from a governmental agency, court of law, regulation, or civil service process. MIND Research Institute also reserves the right to use or disclose any information as needed to fulfill



your requests or to cooperate in any law enforcement investigation or an investigation on a matter of public safety, or the safety of our users or customers; to enforce the Terms of Use, Homeschooling EULA, or this Privacy Policy; to protect the integrity of the Sites and our services; to protect our rights or those of our Users, customers, contractors, or licensors; to investigate, prevent, or take action regarding illegal activities, fraud; to take precautions against liability; to provide evidence in litigation or dispute; or to respond to an emergency.

#### **To parents/legal guardians.**

We may provide Student Records or Student Performance Data to the Students' Parents / legal guardians.

#### **To teachers / LEAs.**

We may provide Student Records and corresponding Student Performance Data to the teachers or other authorized LEA representatives for the applicable Students.

#### **In a business transfer.**

We may transfer personal information and other data in our possession in connection with an acquisition by or merger with another company, if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding.

#### **How do I review, correct, update and / or remove my personal information or my child's personal information?**

MIND Research Institute does not provide, sell, trade, or rent personally identifiable information. We may disclose or share personally identifying information as follows:

#### **Reviewing and updating Student Records.**

Parents, legal guardians, and Students aged 13 and above may review the personally identifying information contained in Student Records and may have us correct any erroneous Student Records. We will terminate use and storage of any personal information contained in Student Records received from the LEA following written notice of termination, unless we have received consent directly from such Student, if aged 13 or above, or the Student's parent or legal guardian otherwise, to store such Student Records. We will terminate use and storage of any personal information contained in Student Records that we have collected for children under 13 following written request from their parent or legal guardian. To exercise these rights, you may contact us at [privacy@mindresearch.org](mailto:privacy@mindresearch.org). To review Student Records for Students under the age of 13, you will be required to authenticate yourself as the Student's parent / legal guardian, teacher, or other authorized LEA representative to receive information about that Student. You agree and acknowledge that the Sites or Software, or features of the Sites or Software, may be inaccessible or inoperable upon removal of Student Records..

#### **Review and updating other User information.**

Visitors may review, update and/or correct your contact or other personal information at any time by sending an e-mail to us at [privacy@mindresearch.org](mailto:privacy@mindresearch.org) and/or notifying the MIND Research Institute of the changes, as applicable. If you have been prompted to provide information to register an account, you will be provided limited access to your account information to update and/or correct the personal information you have supplied.

#### **How does MIND Research Institute protect personal information?**

Our Site has security measures in place to minimize the risk of loss, misuse, and alteration of the information under our control. Your access to the Restricted Pages or other accounts (if you have any) established through MIND Research Institute or the Site is password-protected so that only you have access to that personal information, so keep your password private and secure.

We provide and require training of all of our personnel involved in the handling, usage, or storage of Student Records or other personally identifying information, which training is renewed periodically. This training includes compliance with relevant federal and state legal requirements, including, as a non-limiting example, the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) ("FERPA") and the Children's Online Privacy Protection Act (15 U.S.C. Secs. 6501 – 6506) ("COPPA"). To protect our information technology environment and the data that we store, we take commercially reasonable security measures, implemented with a multi-tier software architecture, that are consistent with standards generally recognized in the industry. Please be aware, however, that despite our efforts, no security measures are perfect or impenetrable. Due to the open nature of the Internet, we cannot guarantee that any of your information stored on our servers, or transmitted to or from a us or a user, will be 100% free from unauthorized access, and we disclaim any liability for any theft or loss of, unauthorized access or damage to, or interception of any data or communications. By using the Site, you acknowledge that you understand and agree to assume these risks.

Whom does this Privacy Policy apply to?

MIND Research Institute requires its employees and agents who access or utilize Student Records or any other personally identifying information of students or of their families to abide by the terms of this Privacy Policy. MIND Research Institute also contractually requires any of its subcontractors or vendors who are accessing or utilizing such data on its behalf to comply with the requirements of this Privacy Policy pertaining to the use and access of such data.

Where does MIND Research Institute host its services?

MIND Research Institute's infrastructure is hosted within the United States. We design and implement our systems to provide resiliency against server, segment, and geographic failure, through the implementation of a clustered redundant architecture that yields highly available service endpoints, which provide resiliency against server, segment, and geographic failure. We utilize service providers whose systems have been certified for compliance with security standards including ISO 27001. We cannot, however, guaranty that systems will never be subject to a security breach, or will be otherwise error-free. Additional information regarding our system availability and security practices is provided below, and for additional questions, please reach us at [privacy@mindresearch.org](mailto:privacy@mindresearch.org).

How does MIND Research Institute protect data?

Unauthorized access of User data is a real risk facing the users of today's electronic information services. MIND Research Institute strives to keep informed of these risks, and we work diligently to combat them. One method of protecting User data is to utilize cryptography to prevent data visibility in the event of its unauthorized access. MIND Research Institute leverages cryptography to protect user data in the following two ways:

**Data in Transit.**

Our services support Transport Layer Security ("TLS") to encrypt User communications (TLS 1.2 or greater and only the strongest ciphers). Data transferred between our Site and its end Users (including credential submission, data uploads, and data downloads) are sent over TLS connections, which protect such data using strong encryption, so that data in transit is kept in a private channel between the intended User and our systems.

**Data at Rest.**

User data that contains personally identifying information, when "at-rest" (i.e., when in storage) is encrypted using industry standard AES-256. There are two types of "at rest" storage:

- **Database.** Database server disk storage is "volume" encrypted (i.e., encrypted at the level of the database).

- **User Files.** User files are individually encrypted before being recorded on long-term, secondary storage systems.

What does MIND Research Institute do with personally identifiable information after the customer relationship has ended?

Personally identifiable information received from a LEA is de-identified or deleted in a reasonable period of time after the relationship between MIND Research Institute and the LEA has been terminated. Personally identifiable information that is voluntarily submitted by a Visitor pursuant to this Privacy Policy may be retained by MIND Research for the purposes described for Visitor data herein, provided that such information may be reviewed, updated or corrected as provided under the applicable sections of this Privacy Policy.

How does MIND Research Institute respond to breaches?

If you correspond with us by e-mail, or using the “contact us” feature on the Site, you should be aware that your transmission might not be secure. We will have no liability for disclosure of your information due to errors or unauthorized acts of third parties during or after transmission. If we believe that the security of User information may have been compromised, we will comply with applicable laws and regulations regarding notice of such breaches. Without limiting the foregoing, we will notify any LEA whose data is affected by such a breach, and will provide any reasonable cooperation to the LEA to notify affected parents / legal guardians in the event of an unauthorized disclosure of student records. You consent to our use of your e-mail address as a means of such notification. Please notify us of any unauthorized use of your password or account or any other breach of security of which you are aware.

What are "cookies" and how does MIND Research Institute use them?

"Cookies" are pieces of information that a web site transfers to your computer's hard drive for record-keeping purposes. Like many sites on the Internet, we use cookies to identify you when you visit the Site. Most web browsers automatically accept cookies, but if you prefer, you can set your computer to not accept cookies. If you do this, however, you may not be able to use some of the features or services we offer on our Site.

Will MIND Research Institute send me unsolicited communications? How do I opt-out?

The MIND Research Institute may use the information it collects to respond to requests for information, to notify you about functionality changes to the web site, or to provide industry and company updates. You may update or modify your information or change your privacy preferences (such as whether you wish to receive promotional offers) at any time by emailing us at [privacy@mindresearch.org](mailto:privacy@mindresearch.org). If you wish to have your name removed from any of our mailing or subscription lists, please write to us at our above address or click the “remove subscription” link set forth in the relevant communication (typically provided at the end of such communication). In the event that you contact us with this request, all reasonable efforts will be taken to ensure that you will not receive any further communications from which you have opted-out in the future.

What should I know about third party sites?

The MIND Research Institute Site may contain links to other web sites. The MIND Research Institute is not responsible for the privacy practices or the content of such third party sites. Use of information on third party sites is governed by the privacy policy of the operator of the site you are visiting. That policy may differ from ours. The MIND Research Institute has no control over such third party sites, and the existence of a link from our Site is not meant to imply any endorsement of these other third party web sites.

How does MIND Research Institute respond to Do-Not-Track signals?



In some cases, third parties may be able to collect information about a user's online activities over time and across different websites when he or she uses our Site or services. Some web browsers may transmit "do-not-track" signals to the websites with which the user communicates. Because of differences in how web browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. Because there currently is no industry standard concerning what, if anything, websites should do when they receive such signals, we currently do not take action in response to these signals.

What constitutes my acceptance of this Privacy Policy?

By using the Site provided by the MIND Research Institute, you expressly consent to the use and disclosure of information as described in this Privacy Policy. Your continued use of the Site after the effective date of any modification to the Privacy Policy will be deemed to be your agreement to the changed terms.

How do I contact MIND Research Institute? What are my information rights?

If you have any questions about this privacy statement, the practices of this Site, your dealings with this Site, or any disclosure of personal information to third parties for direct marketing purposes, you can contact us in the following ways:

MIND Education  
 5281 California Ave, Suite 300  
 Irvine, CA 92617  
 Tel: (949) 345-8700  
 Toll Free: (888) 751-5443  
 Fax: (949) 572-2680  
 Email: [privacy@mindresearch.org](mailto:privacy@mindresearch.org)

- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor \_\_\_\_\_ will X will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide

prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

## 5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
  - (i) the parent or eligible student has provided prior written consent; or
  - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

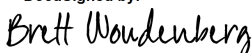
**EXHIBIT D (CONTINUED)****PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 record.
- (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 the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
- (5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the 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/data-privacy-security/report-improper-disclosure>.

**BY THE VENDOR:**

DocuSigned by:



Signature

**Brett Woudenberg**

Brett Woudenberg

**Printed Name****Chief Executive Officer**

CEO

**Title**

5/18/2023

**Date**

**EXHIBIT D (CONTINUED)**

## SUPPLEMENTAL INFORMATION

 ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT  
 BETWEEN  
 ERIE 1 BOCES AND **MIND EDUCATION**

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with **MIND Education** which governs the availability to Participating Educational Agencies of the following Product(s):

**ST Math: K8, ST Math: Gateway, ST Math: Early Learning, ST Math: Summer Immersion, Annual Service & Renewal Fee, ST Math: District Early Learning, ST Math: District Summer Immersion, ST Math: Assessment Support Tool**

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

**Exclusive Purpose for which Protected Data will be Used:** The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: **N/A**

**Duration of MLSA and Protected Data Upon Expiration:**

- The MLSA commences on **July 1, 2023 and expires on June 30, 2026.**
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back



to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

**Data Storage and Security Protections:** Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

**Encryption of Protected Data:** Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

