Title: Executive Director

Address: 355 Harlem Rd

West Seneca, NY 14224

Title: Head of Sales - North america

Address: 228 Park Ave S, #15992, New York, NY, 10003

Date: 6/1/2023

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:

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: Role based access controls and principle of least privilege to restrict access to data, Access and audit logs, Data segregation between environments and services, Security advisory and detection services, Encryption of data at rest and in transit, Isolation of confidential data to production environments, Scrubbing of confidential data when used in non-production, development or test environments, Policies that restrict use or distribution of confidential data, Automated retention policies to minimize storage of data, Policies that require use of access controls and disk encryption on employee devices, Daily test of backups to verify integrity of restoration. See complete Mathspace privacy policy below, and at https://mathspace.co/us/privacy-policy

Protecting the privacy of all individuals, and particularly students, using Mathspace is a priority for us. Details of how we do this are provided below.

Our Privacy Principles

- We are committed to creating a safe and secure online environment for our users.
- We strive to be as open and transparent as possible. We have endeavored to write this policy in a way that is clear and easy to navigate. It is important to us that our users can easily understand the personal information we collect about them and how we protect their privacy.
- We will never sell your personal information to third parties.
- We take the protection of your personal information very seriously, using the best of modern technology feasible for us to protect data and restrict unauthorized access to that information.

Introduction

This Privacy Policy provides important information about the privacy practices of Mathspace Inc. ("Mathspace", "us", or "we") for our website (www.mathspace.co), our associated learning tools and mobile applications.

This Privacy Policy explains how we collect, use, store and disclose the personal information you provide to us as part of your use of our services. With respect to personal information, Mathspace is referring to information which can be used to personally identify a user, such as full name, email address, school name or a photograph.

Collection of Personal Information

We take the information you provide to us very seriously, and we strive to put you in control of decisions around that information. Mathspace collects the following information about you and your use of our services:

Personal information.

When you register for, browse and/or use our services, you may provide Mathspace with "personal information" (such as your full name, email address or a photograph) that can be used to identify you. For School Users, your personal information is also presented to educators in your school or district.

Information about your use of our services and other user-provided information.

We may collect usage information about your use of certain features of our services, such as the number of problems you have attempted, the number of videos you have viewed and the amount of time spent to complete a problem. This enables us to better tailor educational experiences that are most appropriate for you.

Location information.

We may collect and use information about your location (such as your country) to provide you with tailored educational experiences for your region, but we do not collect the precise geolocation of you or your device.

Mathspace uses personal information in the following ways:

To enhance our services and the services we provide.

Mathspace uses the personal information you provide or that we collect to enhance our relationship with you and to operate, maintain, enhance and provide all of the features and services that we provide. Mathspace, for instance, remembers your recent activity so we can recommend the most appropriate content for you on your next visit.

To understand how you and other users use our services.

Mathspace uses any non-personally identifiable information that you provide or that we collect from users in an aggregated format to understand and analyze the usage trends, learning behaviors and preferences of our users, to improve the way our services work and look, and to create new features and functionality.

Ownership of Data for School Users

In addition to presenting student data within our service we provide Schools the ability to download data of student activity on our Services to a CSV file. This data is owned by the School and continues to be the property of and under the control of the School.

Data Retention and Backup

Any user may request a deletion of account details at any time. School administrators may also request a deletion of account details at any time on behalf of their School users. In such cases we will first allow the school to download any data to a CSV file for their ownership. We will then proceed to delete any personal data including names, emails and School name from our database. We will maintain deidentified transactional data for the purposes of improving our adaptive recommendations to all users which is a core part of our service.

For all account deletion requests we may continue to store data on our backup databases for a period of up to 90 days as part of our regular backup processes for restoring user data in case of emergency.

Backup Measures

- Database backups are produced daily by an automated system.
- Database backups are stored encrypted with AES-256.
- Database backups are kept up to 90 days.
- Any data requested to be deleted will be retained for the 90 days of backups only.
- Our Recovery Time Objective is 8 hours and Recovery Point Objective is 24 hours.
- Audit logs for site users are kept only for admin user transactions, and are stored permanently. The elements stored are timestamp, description of changes, and user ID, and kept as a history against each admin user and affected record.
- Audit logs are visible only to admin users. Only engineers are able to access the log storage to delete audit logs.

Our Approach to Data Security

Data security is important to you, and to us.

Mathspace uses a combination of physical, managerial and technical safeguards designed to preserve the integrity and security of your personal information and other information we store in connection with our services. For example, when you enter sensitive information, we encrypt the transmission of that information using secure socket layer technology (SSL) or similar technologies. However, no data transmissions over the internet can be guaranteed to be 100% secure. We take every precaution available to protect all data provided to us in the educational pursuit of digital content.

Mathspace uses Amazon Web Services to host our website, with personal information stored in an encrypted database. Our website is hosted in the United States.

Data Breaches

If we learn of a data security incident that compromises or appears to compromise your personal information, then we will attempt to notify you electronically so that you can take appropriate protective steps. We may also post a notice on our website if a data security incident occurs.

- Data breaches should be reported immediately to the Mathspace support team with full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how many people are involved. Contact details are security@mathspace.co and suppport@mathspace.co.
- Our Data Breach Policy describes a response plan with the following stages:
    - Contain the breach and make a preliminary assessment
    - Evaluate risks associated with the breach
    - Notification of the breach
    - Review and respond to prevent future breaches
- Mathspace will immediately notify affected users and conduct an internal investigation of the breach, and remedy as appropriate. We attempt to respond quickly to any data breach through the following measures:
    - Automated vulnerability scanning will immediately detect changes to files that match malware signatures.
    - Daily code deployment process raises warnings for other unexpected changes to files.

Transmission of Data

All website data is transmitted over HTTPS, with preference for TLS 1.2. Please see our A+ rating with Qualys SSL Server Test: https://www.ssllabs.com/ssltest/analyze.html?d=mathspace.co.

Other protocols in place for backend processes are also always encrypted, and make use of TLS 1.2 or SSLv3.

Technical Security Architecture

Mathspace makes use of the following security architecture to insure data privacy.

- Layered defense approach to security architecture.
- CloudFlare to mitigate against DDOS attacks.
- Web application firewall to detect and prevent common web application attacks and intrusions.
- HTTPS enforced through HSTS and HSTS preload registration.
- Single-sign on for authentication is supported.
- Secured email transmission.
- Automated vulnerability scanning.
- Firewall whitelists are configured to control access to non-public servers.
- Masking and stripping of personal information whenever not strictly required.
- Data is encrypted at rest and in transmission.
- Hosting provider (Amazon Web Services) is ISO 27018 certified and verified by an independent third party assessor.
- User-based and role-based permissions are implemented to restrict access to information as appropriate.
- Penetration testing by an independent third party is conducted on a yearly basis.

Encryption and Authentication Protocols

Data at rest and data in transit

- All data is encrypted in transit and in rest.
- Database storage is encrypted with AWS RDS encryption features.
- Data in transit is secured with HTTPS/TLS 1.2, TLS 1.2 or SSLv3.

Encryption and authentication mechanisms

- All website data is transmitted over HTTPS, with preference for TLS 1.2. (Please see our A+ rating with Qualys SSL Server Test: https://www.ssllabs.com/ssltest/analyze.html?d=mathspace.co.)
- SAML 2.0 through Shibboleth 2.5.2
- Clever Instant Login through custom Django 1.9.3 integration (OAuth 2.0 Authorization Grant flow)
- OAuth 2.0 Authorization Grant flow through custom Django 1.9.3 integration
- Our SSL certificate is signed with RSA 2048 bits (SHA256withRSA). HTTPS enforced through HSTS and HSTS preload registration.
- Protocols in place for backend communication are also always encrypted, and make use of TLS 1.2 or SSLv3.
- Data at rest is encrypted with AES-256 and AWS Key Management Service (KMS) which uses a hardware security module to protect our keys.
- Passwords are stored using the PBKDF2 algorithm with a SHA256 hash and per- user salt. The work factor and algorithm used is frequently updated.
- We do not implement our own encryption or cryptography algorithms.
- SSO-enabled users are authenticated through the SSO mechanisms above - SAML 2.0 or OAuth 2.0 protocols.
- Authorization is managed through a graph-based access control (GBAC) system.

Password Authentication

- SSO-enabled users will not have passwords stored within Mathspace.
- Mathspace users without SSO have their passwords stored using the PBKDF2 algorithm with a SHA256 hash and per-user salt. The work factor and algorithm used is frequently updated.
- Passwords and other credentials are never stored or transmitted in plaintext in the database nor in logs, nor over insecure protocols.
- (SSO-enabled users will not have passwords stored within Mathspace.)
- Passwords must be at least 6 characters long.
- Passwords can’t be entirely numeric.
- Passwords may not be similar to user attributes such as first/last name or email.
- Passwords may not be one of the 1000 most common passwords. Input/Output Controls
- Input controls implemented include error reporting and handling, authorization checks, data consistency checks, and transaction logs.
- Processing controls include data validation checks, completeness checks, checksums, and versioning.
- Output controls include one-time use links, expiration-based links and output logs.

Vulnerability Assessment, Identification, Remediation and Patch Management

- System patches that are security fixes must be applied by a daily automated process.
- Systems must run automated vulnerability and malware scanning software.
- All code changes must be reviewed by another team member.
- All code changes must be scanned by a software security vulnerability scanner.
- Penetration tests performed by an external party must be conducted yearly.
- Issues arising from the above processes must be urgently attended to assess impact and appropriate prioritization

Sharing information with Third Party Service Providers

Mathspace takes great care to protect the personal information you provide to us. We do not sell your personal information to third parties.

This section explains circumstances in which we may share information with third parties.

Functional Purposes

Mathspace uses third-party service providers for customer support, to monitor our website usage, and to monitor the performance of our servers. These third party providers are required for optimal website performance and user experience. Data is not used for marketing purposes.

Advertising Optimisation Purposes

Mathspace does not advertise to any Mathspace Child Users or any individuals under the age of 18 years.

We do use third party service providers to monitor advertising which we deliver to individuals over 18 years of age. We only use these Services for attribution, analytics, market research and ad optimization.

This information is collected directly and automatically by these third parties on adult-directed pages of the website. Mathspace does not participate in these data transmissions. The information collected is anonymous and does not share personally identifiable information with these third parties.

In order to further protect the privacy of our visitors and users, Mathspace chooses not to partake in any retargeting or remarketing advertising campaigns due to the type and nature of personally identifying information collected necessary to run such marketing efforts.

Summary

Except for the purposes provided in our Privacy Policy, Mathspace WILL NOT disclose the information that it obtains from you to third parties without user's express written permission, or where we believe, in good faith, that the law requires us to disclose the information.

Mathspace works with third party service providers with agreements that ensure that our data security and privacy requirements are protected.

Single Sign On Security Protocols

We support a few SSO protocols:

- SAML2.0 through Shibboleth 2.5.2
- SAML2.0 through Shibboleth 2.5.2
- Clever Instant Login through custom Django 1.9.3 integration (OAuth 2.0 Authorization Grant flow)
- OAuth 2.0 Authorization Grant flow through custom Django 1.9.3 integration

Secure Data Exchange

Districts integrate with Clever to sync their data. Districts send a request through Clever to add the Mathspace application, and enable Data Sharing with Mathspace. The district is able to select how much data to share. Mathspace needs teachers, students, sections and schools data, with names. Emails are recommended. Mathspace will then be able to sync the data shared through Clever Secure Sync. Data accessed from Clever is only transmitted through HTTPS/TLS 1.2 encrypted protocols. Mathspace runs a daily automated sync task, as well as can sync on demand.

Alternatively, districts may upload CSV files onto our SFTP server, which can be processed on an automated daily schedule. Districts must provide Mathspace with a public key to initiate an account. Districts must then upload complete CSV files of teachers, students, enrolments, sections and schools with ID, name and email records.

Data accessed from Clever is only transmitted through HTTPS/TLS 1.2 encrypted protocols. Data accessed from our SFTP server is only transmitted through SSL 2/3 encrypted protocols. All access to and from Mathspace servers is through encrypted protocols such as HTTPS or SSL.

Use of Cookies

To provide a personalized learning and high-quality experience for our users, we may use various technologies that automatically record certain technical information from your browser or device, including standard log files, or web beacons. This technical information may include your internet protocol (IP) address, device or browser type, internet service provider (ISP), referring or exit pages, clickstream data, operating system and the dates and times that you visit our website. We do this to better understand how our users are using our website so we can improve site functionality and the services we offer you.

Like most websites, whether or not you are a registered member, we may send one or more cookies – small text files containing a string of alphanumeric characters – to your computer. Cookies remember information about your activities on a website and enable us to provide you with a more personalized learning experience. Mathspace may use both session cookies and persistent cookies. A session cookie disappears automatically after you close your browser. A

persistent cookie remains after you close your browser and may be used by your browser on subsequent visits to our website. You can, however, remove a persistent cookie at any time. Please review your web browser "Help" file to learn the proper way to modify your cookie settings. However, without cookies you will not have access to certain services and features on our website. You will also have the option to opt out of any non-essential cookies.

Accessing or Correcting Your Personal Information

You can access the personal information we hold about you by contacting us using the details set out below (under "Contact Us"). Sometimes, we may not be able to provide you with access to all of your personal information and, where this is the case, we will tell you why. We may also need to verify your identity when you request your personal information. If you think that any personal information we hold about you is inaccurate, please contact us and we will take reasonable steps to ensure that it is corrected.

Changes and Updates to this Privacy Policy

Our Privacy Policy may be updated periodically. Mathspace will contact users via email if any policy change diminishes privacy rights that they were entitled to prior to those policy changes. Please ensure you have added an email address to your Mathspace account if you wish to be notified of any Privacy Policy changes.

Making a Complaint

If you think we have breached any laws relating to privacy, or you wish to make a complaint about the way we have handled your personal information, you can contact us using the details set out below (under "Contact Us"). Please include your name, email address and/or telephone number and clearly describe your complaint. We will acknowledge your complaint and respond to you regarding your complaint within a reasonable period of time. If you think that we have failed to resolve the complaint satisfactorily, we will provide you with information about the further steps you can take.

Contact Us

Mathspace Inc.
228 Park Ave S #15992
New York, NY 10003-1502
support@mathspace.co

Federal Compliance Statements

Children's Online Privacy Protection Act (COPPA)

The student information provided by the district to the Company will be used only for the student's use of the educational program. The information collected will be used strictly for educational purposes and not for any commercial purpose.

Family Educational Rights and Privacy Act (FERPA)

Mathspace complies with all requirements of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)

Protection of Pupil Rights Amendment (PPRA)

Mathspace complies with all requirements of the PPRA.

(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 _✓____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:
Jonathan Templin
EA3631EEBF5F453...
Signature

Jonathan Templin
Printed Name

Head of Sales - North america
Title

6/1/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND MATHSPACE INC

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Mathspace Inc] which governs the availability to Participating Educational Agencies of the following Product(s):

Mathspace

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: Not Applicable - Mathspace will not use subcontractors

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.