Title: Executive Director

Address: 355 Harlem Rd

West Seneca, NY 14224

Title: Partner

Address: 1 E Broad St 130-1006, Bethlehem, PA 18018

Date: 8/30/2023

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: See Exhibit E

(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 [*check one*] _____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:
Peter Schmitt
23C201E0FD094A4...
Signature

Peter Schmitt
Printed Name

Partner
Title

8/30/2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND Right Reason Technologies

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

RightPath Student Success System

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: We will not be utilizing 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.

EXHIBIT E
RIGHT REASON TECHNOLOGIES DATA AND PRIVACY PLAN

Introduction

Right Reason Technologies, LLC (RRT) needs to gather and use certain information about school districts. These can include teachers, students, classes, class rosters, student assignments and grades.

This policy describes how this personal data is secured, stored, and accessed to meet the company's data protection standards and the requirements of its customers.

Why this policy exists

This data protection policy ensures that RRT:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes personally identifiable information
- Protects itself from the risks of a data breach

Responsibilities

Everyone who works for or with RRT shares in the responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The B**oard of Directors** is ultimately responsible for ensuring that RRT meets its legal obligations.

- The IT Manager is responsible for:

    - Keeping the Board of Directors updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data RRT holds.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The general staff is responsible for:

    - Keeping all data secure, by taking sensible precautions and following the guideline below.
    - Using strong passwords never sharing passwords.
    - Securing personal data from unauthorized people, either within the company or externally.
    - Regularly reviewing and updating data, if it is found to be out of date. If no longer required, it will be deleted and disposed of.

- Requesting access to data it from their line managers or requesting help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data will be safely stored. Questions about storing data safely can be directed to the IT manager.

- When not required, the paper or files will be kept **in a locked drawer or filing cabinet**.
- Employees will make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer.
- **Data printouts will be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data will be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these will be kept locked away securely when not being used.
- Data will only be stored on **designated drives and servers** and will only be uploaded to an **approved cloud computing service**.
- Data will be stored in a manner limiting access to those that specifically require the data to perform specific tasks.
- Servers containing personal data will be **sited in a secure location**, away from general office space.
- Data will be **backed up frequently**. Those backups will be tested regularly, in line with the company's standard backup procedures.
- Data will **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data will be protected by **approved security software and a firewall**.

Data Use

The following policies help to ensure that all employees minimize the loss, corruption or theft of personal data.

- When working with personal data, employees will ensure **the screens of their computers are always locked** when left unattended.
- Personal data **will not be shared informally**. In particular, it will never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorized external contacts.
- Personal data will **never be transferred, except between RRT and the client district**. RRT will never transfer personal data to any other entity. It will be transferred to the client district who can then transfer the data to some other entity. The only exception to this rule is where RRT has an agreement with the client district to automate or integrate systems and sends or receives personal data to provide the integration service.
- Personal Data will be destroyed when not needed for a specific use.

Securing Data and Limiting Access

Given the ubiquity of computer use, and subsequently data storage and use, securing data and limiting access requires a multi-faceted approach. In addition to the sections above on Data Storage and Data Access, the RightPath™ application also provides for data security and limiting access.

Access is limited to each device, application, or service that stores data. This access is limited to those that require access to perform a specific duty.

- Access to servers where file data is transferred is only accessible to the team that supports the process of managing loaded data.
- Access to database servers is limited to those that are required to manage the database servers and perform data services.
- Access to other data is all based on the user permissions to specific resources, i.e., file folders on a server or a SharePoint™ site.

RightPath™ Security and Access

- The RightPath™ system supports access over Secure Sockets Layer (SSL) using the HTTPS protocol.
- All users must enter a username and password to access the RightPath™ system.
- All features of the RightPath™ system are secured by specific permissions. Users are provided with permission sets. The permission set for any user can be completely customized, thereby limiting the user's access to specific features of RightPath™.
- Users can also be limited to the specific sets of student data that they can see. RightPath™ supports the ability to allow a specific user to have access to
    - All students,
    - Students within one or more buildings,
    - Students within one or more class sections,
    - No students.
- Right Reason Technologies (RRT) receives data from most of its clients in order to synchronize the RightPath™ system with data typically stored in a Student Management System (SMS). RRT supports a secure FTP (FTPS) solution to provide for secure transfer of data. Each client that utilizes this service is separated from all other clients so that one client district cannot see another client district's data. Additionally, the RightPath system uses web-based REST APIs as another synchronization option which is also secured by HTTPS and passwords.

Third Party Partner Companies

- We share data with third party providers under very limited circumstances.
- We may share data with third-party providers in order to provide a specific feature or service that enhances our overall product. Data may also be shared with third-party providers that provide web-hosting services (for example, Microsoft Azure) or similar technology related services.
- Our third-party providers are not allowed to use shared data for any other purpose other than providing a service to us. We make significant efforts to limit the data that is shared and ensure that our third-party providers follow security practices that meet the needs of our client districts.

Best Practices

RRT employs today's best practices with respect to the data RRT stores, its privacy and protection.

- Encryption
  - RRT supports using SSL for both access to the RightPath™ system and the FTP system for data transmission/integration.
- Firewalls
  - RRT's corporate network is protected from external access via a firewall. All ports are turned off by default. Almost all access requires a VPN connection.
  - RightPath™ production servers hosted at Rackspace are protected by firewalls, which are configured to only allow traffic as needed by the application and support team.
- Server Access
  - The RightPath servers are located in a secured server room.
  - Our RightPath servers are located within a 3rd party hosting provider, Azure. Azure is a leading provider of hosting services and complies with state, federal and local laws pertaining to data privacy.
  - These servers are protected with a firewall such that only necessary ports are opened to the public Internet as to ensure the operation of our application.
  - Network access to these servers is limited by a firewall, as well as username and password. Access to each server is open only for staff with a need to work with a specific server.
- Backups
  - The backups of RightPath data are taken frequently, encrypted, and maintained off-site for disaster recovery. Data transportation for off-site backups is all performed over a secure network.
- Passwords
  - All passwords used by RRT employees are strong passwords. These passwords are enforced by password policies that do not allow the use of weak passwords.
- Access Permissions
  - Please refer back to the sections on Data Storage and Data Use.

Parents' Bill of Rights

Right Reason Technologies is committed to protecting the privacy and security of all student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. RRT wishes to inform Eastern Suffolk BOCES:

1. Personally identifiable information will not be sold or released for any commercial purposes.
2. Personally identifiable information will not be released or transferred to another entity unless it is both approved by the client district and required to provide a specific service as contracted with the client district/LEA.
3. Parents have the right to inspect and review the complete contents of their child's education record as maintained by Right Reason Technologies. Requests must be made through their local district or BOCES.
4. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, are in place when data is stored or transferred. The RightPath™ system supports encryption standards such as HTTPS (application access) and FTPS (for data transfer). Additionally, the RightPath™ system requires password access and allows client districts to customize specific permissions and access to selective subsets of the student population.
5. The list of data elements collected and stored by Right Reason Technologies is available at

   http://support.rightreasontech.com/support/solutions/articles/1000034281-sms-data-loading-specifications

   and further consists of:
   a. Assessment scores that are administered by RRT and stored in the RightPath™ system,
   b. Assessment scores that are provided to us by client districts for analysis and reporting,
   c. Student lessons and grades when the lessons are assigned and graded within the RightPath™ system,
   d. Response to Intervention Tier levels per student, as well as intervention log details created by district staff within the RightPath™ system.

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 directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov