BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Right Reason Technologies, LLC ____
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary □ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	Rightpath synchroizes with district's SMS in order to function properly. It is primarily used for elearning, APPR observations, SLO and End of Year Evaluations, and data reporting.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☑ APPR PII

Contract Term	Contract Start Date 07/01/2023 Contract End Date 06/30/2024
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) □ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. □ Using Contractor owned and hosted solution □ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Rightpath is hosted in Microsoft Azure. It is protected by the policies in our Data and Privacy document. In short, access is limited to staff with specific priviledges, and protected by firewall, and SSL. User access is protected by username/password and encrypted over SSL.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Please see Data Security and Privacy Policy.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please see Data Security and Privacy Policy.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Please see Data Security and Privacy Policy.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Please see Data Security and Privacy Policy.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Please see Data Security and Privacy Policy.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please see Data Security and Privacy Policy.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please see Data Security and Privacy Policy.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please see Data Security and Privacy Policy.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please see Data Security and Privacy Policy.

Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org . (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	David Mehrtens
[Printed Name]	David Mehrtens
[Title]	Partner
Date:	03/14/2023

January 13, 2022

YOUR SOLUTION FOR STUDENT SUCCESS

RIGHT REASON TECHNOLOGIES

Right Reason Technologies

Data Security and Privacy Plan

Contents

Introduction 3

Why this policy exists 3

Responsibilities 4

Data storage 4

Data Use 6

Securing Data and Limiting Access 7

Best Practices 8

Parents’ Bill of Rights .... **Error! Bookmark not defined.**

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.