Gilbertsville - Mount Upton Central School District

693 State Highway 51 • Gilbertsville, New York 13776-1104
Phone (607) 783-2207 • Fax: (607) 783-2254

Annette Hammond, Superintendent
Eric Voorhees, Data Protection Officer

Gilbertsville – Mount Upton Central School District Parents' Bill of Rights for Data Privacy and Security

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or Principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled Student Directory Information (FERPA);

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.pl 2.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx, 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 to Data Protection Officer of;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

    - Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
    - Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
    - The District will require complaints to be submitted in writing;
    - The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:
    - the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;
    - how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);
    - the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed);
    - if and how a parent, student, eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;
    - where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third-party contractor where the third party contractor receives student data or teacher or Principal data.

Instructions for Third-Party Contractors

Please complete the Supplemental Information Details Worksheet and Data Privacy Rider on the next two pages and return them to the Data Protection Officer of Gilbertsville – Mount Upton Central School District:

Eric Voorhees
Technology Director/CIO

Email: evoorhees@gmucsd.org
Phone: (607) 783-2207, extension 126

Gilbertsville – Mount Upton Central School District
693 State Highway 51
Gilbertsville, NY 13776-1104

This Supplemental Information Details Worksheet to be completed by the Third-Party Contractor and returned to Gilbertsville – Mount Upton Central School District

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

X Yes

Please complete Sections 2, 3 and the Data Privacy Rider on the next page

☐ No

Please complete Section 3

Section 2: Supplemental Information Details

Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	To utilize the Software, LEA devices are activated, and students obtain user names and passwords in order to utilize the software. 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.
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	ST Math ensures that any other entity that can access student or teacher data meet or exceed our industry best practices in regards to data protection and security.
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	Once the contract has ended, MIND Research Institute's policy is to de-identify user data on a quarterly basis.
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	In the event that a parent, student, or eligible student contacts MIND to review or challenge the accuracy of data, MIND will refer them back to the School District, who will follow necessary and proper procedures regarding the request. MIND will respond in a reasonably timed manner to the District's request for Student Data in a student's records to view or correct as necessary.

Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	All data collected and stored by ST Math is housed in Amazon Web Services in the United States and encrypted in transit and at rest according to industry best practices that will meet or exceed customer requirements. All access is fully authenticated and authorized using a role based model for all PII data.
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	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

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Gilbertsville – Mount Upton Central School District Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Company Name MIND Research Institute Product Name ST Math

Printed Name Brett Woudenberg Signature Brett E. Woudenberg Date Nov 11, 2022

Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

Gilbertsville – Mount Upton Central School District and the Third-Party Contractor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the Gilbertsville – Mount Upton Central School District's Data Security and Privacy Policy;

3. The Parties agree that the Gilbertsville – Mount Upton Central School District's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

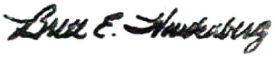
5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
    c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
    e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
    f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
    g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name MIND Research Institute _ Product Name ST Math

Printed Name Brett Woudenberg Signature  Date Nov 11, 2022