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?

☑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)	McGraw Hill uses PII to provide the requested service or to process transactions such as information requests or purchases in order to meet our contractual obligations to you. We will also process your PII to meet our legitimate interests, for example to personalize your experience and to deliver relevant content to you; to maintain and improve our services; to generate and analyze statistics about your use of the services; and to detect, prevent, or respond to fraud, intellectual property infringement, violations of law, violations of our rights or Terms of Use, or other misuse of the services. Except as described in this notice, we limit the use, collection, and disclosure of your PII to deliver the service or information requested by you. We do not collect, use, or disclose PII that is not reasonably related to the purposes described within this notice without prior notification. Your information may be combined in an aggregate and de-identified manner in order to maintain and/or improve our services.
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)	McGraw Hill requires any and all subcontractors, persons or entities with which the Contractor may share the PII to commit contractually that they will abide by the terms of the Agreement and/or the data protection and security requirements set forth in Education Law §2-d.
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)	When the Agreement terminates between the District and the McGraw Hill, upon written request, McGraw Hill shall return to the District or, if agreed to by the District, destroy the remaining PII that McGraw Hill still maintains in any form.
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)	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify McGraw Hill. McGraw Hill agrees to facilitate such corrections within 30 days of receiving the District's written request.

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 is stored in the continental United States on AWS servers. McGraw Hill utilizes the most up-to-date security systems and 24/7 monitoring. McGraw Hill also has very strict internal processes to safeguard customers' data, and all applications are built in compliance with federal regulations including FERPA. System penetration testing, vulnerability management and intrusion prevention is managed in conjunction with our third party infrastructure provider. The application logs security-relevant events, including information around the user, the date/time of the event, type of event, success or failure of the event, and the seriousness of the event violation. User authentication communication and storage is protected by 256-bit advanced encryption standard security.
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	Data will be encrypted while in motion and at rest.

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 McGraw Hill LLC Product Name all instructional materials provided by McGraw Hill

Printed Name Kimberly Harvey Signature Kimberly A. Harvey Date 09/16/2024

McGraw Hill Data Privacy and Security Guidelines

This Data Privacy and Security Guidelines (**"DPSG"** or **"Security Guidelines"**) document sets forth the duties and obligations of McGraw Hill (defined below) with respect to Personal Information (defined below). In the event of any inconsistencies between the DPSG and the Agreement (defined below), the parties agree that the DPSG will supersede and prevail. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions.

    a. **"Agreement"** means the Agreement for the Services between the McGraw Hill LLC entity (**"McGraw Hill"**) and Subscriber incorporating the Privacy Notice to which these Security Guidelines are referenced and made a part thereof.

    b. **"Applicable Laws"** means federal, state and international privacy, data protection and information security-related laws, rules and regulations applicable to the Services and to Personal Information.

    c. **"End User Data"** means the data provided to or collected by McGraw Hill in connection with McGraw Hill's obligations to provide the Services under the Agreement.

    d. **"Personal Information"** means information provided to McGraw Hill in connection with McGraw Hill's obligations to provide the Services under the Agreement that (i) could reasonably identify the individual to whom such information pertains, such as name, address and/or telephone number or (ii) can be used to authenticate that individual, such as passwords, unique identification numbers or answers to security questions or (iii) is protected under Applicable Laws. For the avoidance of doubt, Personal Information does not include aggregate, anonymized data derived from an identified or identifiable individual.

    e. **"Processing of Personal Information"** means any operation or set of operations which is performed upon Personal Information, such as collection, recording, organization, storage, use, retrieval, transmission, erasure or destruction.

    f. **"Third Party"** means any entity (including, without limitation, any affiliate, subsidiary and parent of McGraw Hill) that is acting on behalf of, and is authorized by, McGraw Hill to receive and use Personal Information in connection with McGraw Hill's obligations to provide the Services.

    g. **"Security Incident"** means a confirmed, unsecured, unlawful access to, acquisition of, disclosure of, loss, or use of Personal Information which poses a significant risk of financial, reputational or other harm to the affected End User or Subscriber.

    h. **"Services"** means any services and/or products provided by McGraw Hill in accordance with the Agreement.

2. Confidentiality and Non-Use; Consents.

    a. McGraw Hill agrees that the Personal Information is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement or this DPSG, McGraw Hill shall not Process Personal Information for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.

    b. McGraw Hill shall maintain Personal Information confidential, in accordance with the terms set forth in this Security Guidelines and Applicable Laws. McGraw Hill shall require all of its employees authorized by McGraw Hill to access Personal Information and all Third Parties to comply with (i) limitations consistent with the foregoing, and (ii) all Applicable Laws.

    c. Subscriber represents and warrants that in connection with any Personal Information provided directly by Subscriber to McGraw Hill, Subscriber shall be solely responsible for (i) notifying End

Users that McGraw Hill will Process their Personal Information in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.

3. Data Security.

   McGraw Hill shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of Personal Information. McGraw Hill's security measures include the following:

   a. Access to Personal Information is restricted solely to McGraw Hill's staff who need such access to carry out the responsibilities of McGraw Hill under the Agreement.

   b. Access to computer applications and Personal Information are managed through appropriate user ID/password procedures.

   c. Access to Personal Information is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such Personal Information).

   d. Data is encrypted in transmission (including via web interface) and at rest at no less than 256-bit level encryption.

   e. McGraw Hill or a McGraw Hill authorized party performs a security scan of the application, computer systems and network housing Personal Information using a commercially available security scanning system on a periodic basis.

4. Security Incident.

   a. In the event of a Security Incident, McGraw Hill shall (i) investigate the Security Incident, identify the impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to Subscriber or individuals affected by the Security Incident that McGraw Hill is required by law, subject to applicable confidentiality obligations and to the extent allowed and/or required by and not prohibited by Applicable Laws or law enforcement.

   b. Except to the extent prohibited by Applicable Laws or law enforcement, McGraw Hill shall, upon Subscriber's written request and to the extent available, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

5. Security Questionnaire.

   Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill shall respond to security questionnaires provided by Subscriber, with regard to McGraw Hill's information security program applicable to the Services, provided that such information is available in the ordinary course of business for McGraw Hill and it is not subject to any restrictions pursuant to McGraw Hill's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise McGraw Hill's confidentiality obligations and/or legal obligations or privileges. Additionally, in no event shall McGraw Hill be required to make any disclosures prohibited by Applicable Laws. All the information provided to Subscriber under this section shall be Confidential Information of McGraw Hill and shall be treated as such by the Subscriber.

6. Security Audit.

   Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill's data security measures may be reviewed by Subscriber through an informal audit of policies and procedures or through an independent auditor's inspection of security methods used within McGraw Hill's infrastructure, storage, and other physical security, any such audit to be at Subscriber's sole expense and subject to a mutually agreeable confidentiality agreement and at mutually

agreeable timing, or, alternatively, McGraw Hill may provide Subscriber with a copy of any third party audit that McGraw Hill may have commissioned.

7. Records Retention and Disposal.

    a. Subscriber may access, correct, and delete any Personal Information in McGraw Hill's possession by submitting McGraw Hill's Personal Information Request Form: https://www.mheducation.com/privacy/privacy-request-form.

    b. McGraw Hill will use commercially reasonable efforts to retain End User Data in accordance with McGraw Hill's End User Data retention policies.

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 ("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) De-identified, aggregated, or otherwise anonymized data derived from the above data is not considered to be PII;

2. Confidentiality of all Protected Information shall be maintained in accordance with applicable 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 the requirements of 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, with the understanding that the Vendor also retains aggregate, deidentified, anonymized information for improvement, research, and development 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 as provided by District; 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 McGraw Hill LLC Product Name all instructional materials provided by McGraw Hill

Printed Name Kimberly Harvey Signature Kimberly A. Harvey Date 09/16/2024