

**DATA SHARING AND CONFIDENTIALITY AGREEMENT**  
**INCLUDING**  
**Bill of Rights for Data Privacy and Security**  
**AND**  
**Vendor Information Regarding Data Privacy and Security**

This Data Sharing and Confidentiality Agreement (the “Agreement”) is made and entered into by and between McGraw Hill LLC (the “Vendor”) and The Enlarged City School District of Middletown.

**WHEREAS**, The Enlarged City School District of Middletown and Vendor are parties to a contract or other written agreement (the “Contract”) pursuant to which the Vendor will receive student data and/or teacher or principal data (“Protected Data”) that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from The Enlarged City School District of Middletown for purposes of providing certain products or services to The Enlarged City School District of Middletown; and

**WHEREAS**, both The Enlarged City School District of Middletown and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

**NOW THEREFORE**, in consideration of the mutual promises and covenants contained in the Contract, as well as, this Agreement the parties hereto mutually agree as follows:

**1. Confidentiality**

- a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided for in the Agreement is deemed confidential information.
- b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with **all applicable** federal and state law and that any information obtained will not be revealed to any persons, firms or organizations.

**2. Data Protections and Internal Controls**

- a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by The Enlarged City School District of Middletown that directly relate to a student(s) (hereinafter referred to as “education record”).
- b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:
  1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and
  2. Not use the education records for any other purpose than those explicitly authorized in the Contract and/or Agreement; and

3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and
4. To use encryption technology to protect Protected Data in its custody while in motion or at rest, 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.

### **3. Data Security and Privacy Plan**

- a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from The Enlarged City School District of Middletown.
- b. Vendor understands and agrees that it is responsible for submitting a Data Security and Privacy Plan to The Enlarged City School District of Middletown prior to the start of the term of the Agreement, and it shall:
  1. Outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with The Enlarged City School District of Middletown's policy on data security and privacy, as adopted.
  2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from The Enlarged City School District of Middletown under the Contract.
  3. Outline the training requirement established by the Vendor for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

### **4. Notice of Breach and Unauthorized Release**

- a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:
  1. ~~Immediately~~ **Promptly** Notify The Enlarged City School District of Middletown 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 authorized release.
  2. Advise The Enlarged City School District of Middletown as to the nature of the breach and steps Vendor has taken to minimize said breach.
- b. In the case of required notification to a parent or eligible student, the Vendor shall:
  1. Promptly reimburse The Enlarged City School District of Middletown for the full costs of such notification.

c. Vendor will cooperate with The Enlarged City School District of Middletown and provide as much information as possible directly to The Enlarged City School District of Middletown about the incident, including but not limited to:

1. The description of the incident;
2. The date of the incident;
3. The date Vendor discovered or was informed of the incident;
4. A description of the types of Protected Data involved;
5. An estimate of the number of records affected;
6. The schools within The Enlarged City School District of Middletown affected;
7. 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
8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

ci. The Vendor shall indemnify and hold The Enlarged City School District of Middletown harmless from any ~~third-party~~ claims arising from its ~~Vendor's direct~~ breach ~~within~~ of the Data Sharing and Confidentiality Agreement confidentiality and data security and privacy standards provision.

cii. Vendor acknowledges that upon initial notification from Vendor, The Enlarged City School District of Middletown, 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 agrees not to provide this notification to the CPO directly unless requested by The Enlarged City School District of Middletown or otherwise required by law. 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 The Enlarged City School District of Middletown, Vendor will promptly inform The Enlarged City School District of Middletown of the same.

## **5. Vendor Information**

Vendor understands that as part of The Enlarged City School District of Middletown's obligations under New York Education Law Section 2-d, Vendor is responsible for providing The Enlarged City School District of Middletown with Vendor information (see Vendor Information for Data Privacy and Security) to include:

- a. Exclusive purposes for which the student data will be used;

- b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;
- c. That student data will be returned or destroyed upon expiration of the Agreement;
- d. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and
- e. Where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

## **6. Termination or Expiration of Contract and/or Agreement**

- a. Upon termination of the Agreement, **upon written request** Vendor shall return or destroy all confidential information obtained in connection with the services provided therein and/or student data **upon The Enlarged City School District of Middletown's written request or absent such request, according the Vendor's standard data retention policy**. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement.
- b. If requested by The Enlarged City School District of Middletown, Vendor will assist The Enlarged City School District of Middletown in exporting all Protected Data previously received back to The Enlarged City School District of Middletown for its own use, prior to deletion, in such formats as may be requested by The Enlarged City School District of Middletown.
- c. In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with The Enlarged City School District of Middletown as necessary to transition Protected Data to the successor Vendor prior to deletion.
- d. 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 The Enlarged City School District of Middletown with a certification from an appropriate officer that these requirements have been satisfied in full.

## **PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

The Enlarged City School District of Middletown is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, The Enlarged City School District of Middletown informs the school 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 New York State is available for public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to The Enlarged City School District of Middletown Data Privacy Officer, 223 Wisner avenue, Middletown, NY, 10940. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>

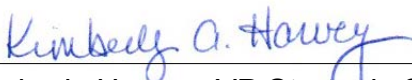
### **Supplemental Information Regarding Third-Party Contractors**

In the course of complying with its obligations under the law and providing educational services to District residents, the Enlarged City School District of Middletown has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) 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;
- 2) 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 laws and regulations (e.g., FERPA; Education Law Section 2-d);
- 3) 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/or whether, when, and how the data will be destroyed);
- 4) 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;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first written above.

  
\_\_\_\_\_  
Kimberly Harvey, VP Strategic Services  
Authorized Vendor Signature

11/15/2024  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Authorized Enlarged City School District of  
Middletown Signature

\_\_\_\_\_  
Date

## VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: McGraw Hill LLC

Product: Instructional Digital Materials

Collects: ☒ Student Data      ☐ Teacher or Principal Data      ☐ Does not collect either

Educational agencies including The Enlarged City School District of Middletown are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

### Part 1: Exclusive Purposes for Data Use

The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:

*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.*

### Part 2: Subcontractor Oversight Details – Select the appropriate option below.

☐ This contract has no subcontractors.

☒ This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law:

*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.*

### Part 3: Contract Lifecycle Practices

The contract expires on 12/31/2025 unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, protected data will be deleted by the contractor, via shredding, returning of data, mass deletion, and upon request, may be exported for use by SA before deletion.

*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.*

### Part 4: Student Educational Records / Improper Disclosure

A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website.

B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.

*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.*

#### **Part 5: Security Practices**

A. Protected data provided to the contractor will be stored: (include *where* and *how*)

*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.*

B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include: *Data will be encrypted while in motion and at rest.*

#### **Part 6: Encryption Practices**

☒ By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).

  
Authorized Vendor Signature

11/15/2024

Date



## 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.