Supplemental Agreement between the

Hampton Bays Union Free School District

and

McGraw Hill LLC

Supplemental Agreement dated December 7, 2023 between the Hampton Bays Union Free School District (the "District"), located at 86 Argonne Rd E, Hampton Bays, NY 11946, and McGraw Hill LLC (hereafter referred to as the "Contractor") located at 8787 Orion Place, Columbus, Ohio 43240.

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the "Agreement") whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d (hereinafter "Supplemental Agreement").

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter "Regulations").

a. "Educational Agency" shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Hampton Bays Union Free School District.

b. "Third Party Contractor" shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs, and in reference to the party to this Agreement shall mean the contractor.

c. "Student" means any person attending or seeking to enroll in an Educational Agency.

d. "Student Data" means Personally Identifiable Information of a "Student."

e. "Eligible Student" means a Student who is eighteen years or older.

f. “Parent” means a parent, legal guardian, or personal in parental relation to a Student.

g. “Building Principal” or “Principal” means a building principal subject to annual performance evaluation review under Education Law §3012-c.

h. “Classroom Teacher” or “Teacher” means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. “Teacher or Principal Data” means Personally Identifiable Information from the records of an Educational Agency 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.

j. “Personally Identifiable Information” shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security can be found as a separate document at the end of this agreement.

<u>EDUCATION LAW 2-d RIDER</u>

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents’ “Bill of Rights” relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency’s Parents’ Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents’ Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between Hampton Bays Union Free School District (“DISTRICT”) and McGraw Hill LLC to the contrary, the contractor agrees as follows:

The contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. The contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. The contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, the contractor shall have in place sufficient internal controls to ensure that the DISTRICT's and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act, Family Educational Rights and Privacy Act ("FERPA") and Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the DISTRICT and/or a Participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the DISTRICT and/or its Participants as that term is defined in §99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the DISTRICT and/or its Participants 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.

The contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, the contractor agrees to comply with the DISTRICT policy(ies) on data security and privacy. The contractor shall promptly reimburse DISTRICT and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by McGraw Hill LLC, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, upon written request, the contractor shall return all of DISTRICT and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

The contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of DISTRICT and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of DISTRICT Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights

applies to the contractor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the contractor's policy on data security and privacy.

3. An outline of the measures taken by the contractor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how the contractor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how the contractor will ensure that any subcontractors, persons or entities with which the contractor will share Protected Data, if any, will abide by the requirements of the contractor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA PRIVACY AND SECURITY PLAN

1. Attached hereto as Exhibit "B" is a copy of the contractor's Data and Privacy Plan with an outline of required supplemental information provided below.

2. Attached hereto as Exhibit "C" is a copy of the District's Bill of Rights.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the District has developed the following "supplemental information" for the Agreement with the Contractor:

a. Student Data and/or Teacher or Principal Data which the Contractor comes into possession as part of its Agreement with the District shall be used for the following exclusive purpose(s): [*Attach the purpose(s) for which the contractor will use the data*].

Contractor 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.

b. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, this Supplemental Agreement, and the data protection and security requirements set forth in Education Law §2-d and Part 121 of the Regulations.

c. The duration of this agreement coincides with the duration of the parties' underlying Agreement. When the Agreement between the District and the Contractor expires or terminates, the Contractor shall [*Attach what will happen to the Student Data or Teacher or Principal Data when the contract expires. For example: "return to the District all remaining Student Data and/or Principal or Teacher Data or, if agreed to by the District, destroy the remaining Student Data and/or Principal or Teacher Data that the Contractor still maintains in any form."*]

When the Agreement terminates between the District and the Contractor, upon written request, the Contractor shall return to the District or, if agreed to by the District, destroy the remaining PII that the Contractor still maintains in any form.

d. [*Attach whether and, if so, how a Parent, Student, Eligible Student, Teacher or Principal may challenge the accuracy of the Student Data and/or Principal or Teacher data that is collected. For example, "Any challenges concerning the accuracy of Student Data and/or Principal Data shall be handled directly between the District and the Parent, Student, Eligible Student, Teacher or Principal. The Contractor agrees to abide by the outcome of such challenges and make any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data as determined by the District." or "The Contractor and District agree to notify the other party of any challenge to the accuracy of Student Data and/or Principal Data. The District and Contractor agree that the party who is responsible for the development of the Student Data and/or Principal Data shall make the final determination with regard to any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data.*]

Parents, students, eligible students, 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 Contractor. Contractor agrees to facilitate such corrections within 30 days of receiving the District's written request.

e. The District and the Contractor hereby agree that the Student Data and/or Principal or Teacher Data shall be stored in the following manner: [*Attach (i) a description of where Student Data and/or Principal or Teacher Data will be stored, described in a manner to* *protect data security, (ii) a description of the security protections taken to ensure Student Data and/or Principal or Teacher Data will be protected and data security and privacy risks are mitigated; and (ii) a description of how the Student Data and/or Principal or Teacher Data will be protected using encryption while in motion and at rest.*]

All data is stored in the continental United States on AWS servers.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement with the understanding that the Contractor also retains aggregate, deidentified, anonymized information for improvement, research and development purposes;

c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental 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 a notice of the disclosure to the State Education Department, District 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 the statute or court order.

d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

6. Breach and unauthorized release of Personally Identifiable Information:

a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any confirmed breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.

b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

McGraw Hill LLC

By: Kimberly A. Harvey

Print Name: Kimberly Harvey

HAMPTON BAYS UNION FREE SCHOOL DISTRICT

By: Michael T Carlson

Print Name: Michael T Carlson

Title: VP, Strategic Services	Title: Asst. Supt. for Curr. & Inst.
Date: December 7, 2023	Date: 12/7/23

Exhibit B

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.

Exhibit C

HAMPTON BAYS UNION FREE SCHOOL DISTRICT

Parents' Bill of Rights for Data Privacy and Security

The Hampton Bays Union Free School District (HBUFSD) is committed to ensuring student privacy in accordance with local, state and federal regulations and district policies. To this end and pursuant to U.S. Department of Education (DOE) regulations (Education Law §2-d), the district is providing the following Parents' Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial or marketing purposes and will be disclosed only as necessary to achieve educational purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record, for more information about how to exercise this right, see HBUFSD Board of Education policy 5500.R.
3. State and federal laws protect the confidentiality of PII and safeguards associated with industry standards and best practices, including but not limited to, employee PII training, use of encryption, firewalls and password protection, must be in place when data is stored, in motion 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. Parents may also obtain a copy of this list by writing to the New York State Education Department (NYSED) via the contact information below.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Hampton Bays UFSD
   Michael T Carlson
   Asst. Supt., Curriculum & Instruction
   86 Argonne Road East
   Hampton Bays, NY 11946
   E-mail: dataprivacy@hbschools.us
   Phone: 631-723-2100

   or

   Chief Privacy Officer,
   New York State Education Department
   Education Department
   89 Washington Avenue
   Albany, New York 12234
   E-mail: privacy@nysed.gov
   Phone: 518-474-0937

6. In the event of a data breach or unauthorized disclosure of students' PII, third party contractors are required by law to notify HBUFSD within seven (7) days of discovery of the breach or unauthorized disclosure. Upon receipt of such notice, the District will utilize multiple means of communication including but not limited to email, phone calls and text messages to notify the public.
7. Contractors that receive PII will be responsible for submitting supplemental agreements addressing statutory and regulatory data privacy and security requirements.

CONTRACTOR:	McGraw Hill LLC
[Signature]	Kimberly A. Harvey
[Printed Name]	Kimberly Harvey
[Title]	VP, Strategic Services