BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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

Name of Contractor	McGraw Hill LLC _____
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	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.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

PDFfiller Document ID: F30F-7D76-59B0-0000

Contract Term	Contract Start Date 09/01/2026 Contract End Date 08/31/2027
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☐ Using a cloud or infrastructure owned and hosted by a third party. ☑ Using Contractor owned and hosted solution ☑ Other: All data is stored in the continental United States on AWS servers. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: 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**
Encryption	Data will be encrypted while in motion and at rest.

PDFfiller Document ID: F30F-7D76-59B0-0000

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	McGraw Hill will limit internal access to education records to individuals who have a legitimate educational interest in such records. McGraw Hill will not use educational records for any other purpose than those explicitly authorized in the contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	McGraw Hill has strict internal processes to safeguard customers' data. Applications are built in compliance with federal regulations including FERPA. McGraw Hill, Inc. digital product resides in AWS, which is physically located in Amazon's
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	McGraw Hill will provide training on requirements of federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	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.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	McGraw Hill will notify District of any confirmed breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	When the agreement terminated 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.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Data is currently stored until a district/account requests in writing data is deleted. McGraw Hill has the ability to properly delete data, when requested by the customer, at any time.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor's data security and privacy program/practices align with NY Ed Law 2-d.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please see NIST CSF Table Data in additional information section below.

Additional Information (More information can be provided at the bottom 2 pages):

PDFfiller Document ID: F30F-7D76-59B0-0000

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

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

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

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

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

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

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

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

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

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

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

CONTRACTOR	
[Signature]	
[Printed Name]	Kimberly Harvey
[Title]	VP Strategic Services, McGraw Hill LLC
Date:	09/04/2026

Version: 4/30/25

PDFfiller Document ID: F30F-7D76-59B0-0000

Additional Information:

McGraw Hill LLC requests edits to the following two sections in order to stay consistent with our company policies and procedures:

Data Transition and Secure Destruction: please update to:

Upon WRITTEN REQUEST FOLLOWING expiration or termination of the Contract, Provider shall: (1) Securely transfer data to the School District, or a successor provider at the School District's option and written discretion, in a format agreed to by the parties, and (2) Securely delete and destroy data.

Challenges to Data Accuracy: please update to:

...Provider agrees to facilitate such corrections within 30 days of receiving the School District's written request.

In the Secure Storage and Data Security section, we could not include our full response in the space allotted. The full response should read:

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.

Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII: we could not include our full response in the space allotted. The full response should read:

McGraw Hill has strict internal processes to safeguard customers' data. Applications are built in compliance with federal regulations including FERPA. McGraw Hill, Inc. digital product resides in AWS, which is physically located in Amazon's datacenters, which are all SOC 2 compliant.

NIST CSF Table Data:

IDENTIFY (ID)
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. ALIGNED. MH UTILIZED CENTRALIZED SYSTEMS SUCH AS CMDB AND WORKDAY TO MANAG E PERSONNEL AND SYSTEMS.

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles , responsibilities, and risk management decisions. ALIGNED.

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understo od and inform the management of cybersecurity risk. ALIGNED

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. ALIGNED. MH HAS A CENTRALIZED CYBERSECURITY FUNCTION RESPONSIBLE FOR THE SECURITY OF THE ENTIRE ENTERPRISE AND ITS MULTIFAC ETED OPERATIONS.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. ALIGNED.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. ALIGNED

PROTECT (PR):
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. ALIGNED. MH PRACTICES ROLE-BASED ACCESS CONTROL (RB AC) AND PRINCIPLE OF LEAST PRIVILEGE (PoLP) ON ALL CRITICAL SYSTEMS AND FACILITIES. ALL ACCESS IS CENTRALLY LOGGED AND MONITORED 24X7.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related dut ies and responsibilities consistent with related policies, procedures, and agreements. ALIGNED. CYBERSECURITY ATTESTATIONS ARE PERFORMED ANNUALLY; AWARE NESS AND TRAINING SESSIONS ARE PERFORMED ENTERPRISE-WIDE MORE FREQUENTLY THROUGHOUT THE YEAR. FOR THE CYBERSECURITY TEAM SPECIFICALLY , ANNUAL TRAINING AND CERTIFICATIONS ARE OBTAINED IN ORDER TO INCREASE SKILLSET AND MAINTAIN CSPS. MANY MEMBERS ON THE CYBERSECURITY TEAM ARE SANS CERTIFIED.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of info rmation. ALIGNED.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordinat ion among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. ALIGNED. ALL SECURITY PO LICIES AND STANDARDS ARE POSTED INTERNALLY.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. ALIGNED.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, proc edures, and agreements. ALIGNED.

DETECT (DE)

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. ALIGNED. ANOMALOUS ACTIVITY IS STILL INVESTI GATED IN THE EVENT IT CORRELLATES WITH OTHER EVENTS WITHIN THE ENVIRONMENT.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measu res. ALIGNED. SECURITY EVENTS ARE MONITORED 24X7 BY OUR ONSHORE AND OFFSHORE SECURITY OPERATIONS CENTER (SOC).

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. ALIGNED. STA NDARD OPERATING PROCEDURES ARE IN PLACE FOR EACH ALERT TYPE.

PDFfiller Document ID: F30F-7D76-59B0-0000

Additional Information:

RESPOND (RE):
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. ALIGNED. STANDARD OPERATING PROCEDURES ARE IN PLACE WITH SLAS AND THE OVERALL DETAILED PROCESS.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). ALIGNED.

Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities. ALIGNED.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. ALIGNED. STANDARD OPERATING PROCEDURES ARE IN PLACE WHICH INCLUDE STEPS FOR CONTAINMENT.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. ALIGNED. LESSONS LEARNED ARE DOCUMENTED AND INCORPORATED

RECOVER (RC):
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. ALIGNED. STANDARD OPERATING PROCEDURES ARE IN PLACE WITH SLAS AND THE OVERALL DETAILED PROCESS.

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. ALIGNED.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). ALIGNED.

PDFfiller Document ID: F30F-7D76-59B0-0000