

EXHIBIT B

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
Description of the purpose(s) for which Contractor will receive/access PII	Classroom Education
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>07/01/2024</u> Contract End Date <u>06/30/2025</u>
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. <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract and EA's written request , Contractor shall: <ul style="list-style-type: none"> • 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 30 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)

	<input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input checked="" type="checkbox"/> Contractor owned and hosted solution. <input checked="" type="checkbox"/> 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: Information is only accessed by those necessary to perform Contractor obligations 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.
Encryption	Data will be encrypted while in motion and at rest.

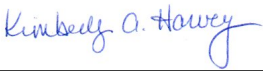
CONTRACTOR McGraw Hill LLC	
[Signature] _____	
[Printed Name]	Kimberly Harvey
[Title]	VP Strategic Services
	1/28/2025

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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 those 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 with the understanding that the Contractor also retains aggregate, deidentified, anonymized information for improvement, research, and development purposes; McGraw Hill will not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student as provided by the District; or (ii) unless required by statute or court order and the third-party contractor provides a 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 the statute or court order.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	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.
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 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.
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 vl.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 - NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan_ Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template_ To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated_ Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework> Please use additional pages if needed_

Function	Category	Contractor Response
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 utilizes centralized systems such as CMDB and WorkDay to manage 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 understood 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 multifaceted 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.

Function	Category	Contractor Response
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 (RBAC) 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 duties and responsibilities consistent with related policies, procedures, and agreements.	Aligned. Cybersecurity attestations are performed annually; awareness 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 information.	Aligned.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Aligned. All security policies 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, procedures, 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 investigated in the event it correlates 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 measures.	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. Standard Operating Procedures are in place for each alert type.

Function	Category	Contractor Response
RESPOND (RS)	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 into SOPs.
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.

Exhibit C.2

McGraw Hill LLC 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 the unlawful access to, acquisition of, disclosure of, loss, or use of Personal Information.
- 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. Data Security Breach.

- a. In the event of a confirmed 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.
- c. McGraw Hill will use commercially reasonable efforts to regularly back up the Subscriber and End User Data and retain any such backup copies for a minimum of 12 months.

EXHIBIT A: DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

**Forestville Central School District Bill of Rights for Data Security and Privacy and
Supplemental Information about a Master Agreement between
Forestville Central School District and McGraw Hill LLC**

1. Purpose

(a) **Forestville Central School District** (herein after "District") and McGraw Hill LLC (hereinafter "Vendor") are parties to a contract, Terms of Service, or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal 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 District for purposes of providing certain products or services to the District (the "Master Agreement").

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between **Forestville Central School District** and **Vendor** that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect

×

at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policies on data security and privacy.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy **that is provided to Vendor in writing**.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between **Forestville Central School District** and **Vendor**". Vendor's obligations described within this section include, but are not limited to:

- i. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and
- ii. its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon **written request from the District at the** termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any **confirmed** breach or unauthorized release of Protected Data it has received from the District 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 unauthorized release.

(b) Vendor will provide such notification to the District by contacting **the current contact on file for the District or Wesley Wright, Director of Technology**, directly by email at **wwright@forestville.com** or by calling **716-965-6565**.

(c) Vendor will cooperate with the District and provide as much information as possible directly to **Wesley Wright** or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, 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 contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, 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 District 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 District, Vendor will promptly inform **Wesley Wright** or his/her designee.

6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached **with the understanding that Vendor also retains aggregate, deidentified, anonymized information for improvement, research and developmental purposes.**

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

- (i) ~~the parent or eligible student~~ the District has provided prior written consent; or
- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) 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 U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy as provided by District, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any confirmed breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

FORESTVILLE CENTRAL SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Forestville School District 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 District 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/student-data-privacy/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 have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.

APPENDIX

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 Forestville School District 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);

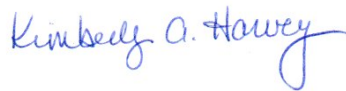
- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, 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.

Adopted: 12/3/2020

BY THE VENDOR: McGraw Hill LLC

Name (Print) Kimberly Harvey

Title: VP Strategic Services



Signature

Date: 1/28/2025