EDUCATION LAW 2-d RIDER

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 Powtoon Ltd (the "Contractor") 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 the Shoreham-Wading River Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. 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. 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. 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, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by New York State ("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. 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 as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2. 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, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information 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.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;
b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. 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; and
e. Where the student data or teacher or principal 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.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of

the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Mr. Gerard Poole
Shoreham-Wading River Central School District
250B Rt. 25A
Shoreham, NY 11786

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected 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. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: **Powtoon Ltd**

Signature: ______________________________ **Date:** **11-JUN-2025**

Printed Name: FEMI ONANUGA **Title:** **DEPUTY CISO**

EXHIBIT “A”

Shoreham-Wading River Central School District
Parents’ Bill of Rights

Parents and guardians of students attending or seeking to enroll in the Shoreham-Wading River CSD are advised that they have the following rights with regard to student data under New York State Education Law.

1. A student’s personally identifiable information will not be released or sold by the District for any commercial purposes.

2. A parent or guardian has 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. Third Party contractors are required to employ technology, safeguards, and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by New York State is available for public review at https://www.nysed.gov/data-privacy-security/student-data-inventoryor by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. 89 Washington Avenue Albany, NY 12234

Complaints should be addressed to:

Alan Meinster, Assistant Superintendent for Curriculum, Instruction, and Assessment; DPO
250B Route 25A
Shoreham, NY 11786
(631) 821-8100
Or with NYSED
Chief Privacy Officer
New York State Education Department
Email: Privacy@nysed.gov

6. This Bill of Rights will be included with every contract entered by the District with an outside contractor if the contractor will receive student, teacher, or principal data. This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student, teacher, or principal data, including the exclusive purpose (s) for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.

7. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

8. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, the District will notify the public via written notice, electronic notice through the District's electronic communication platform, or Telephone notification.

9. 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.

10. Parents may access the State Education Department's Parent's Bill of Rights at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Contractor: **Powtoon Ltd**

Signature: ______________________________ **Date:** **11-JUN-2025**

Printed Name: **FEMI ONANUGA** **Title:** **DEPUTY CISO**

EXHIBIT "B"

Contractor's Supplemental Information

Name of Contractor	**Powtoon Ltd**
Description of the purpose(s) for which Contractor will receive/access PII	In order to allow access and communicate the capabilities and to deliver transactional; email messages, personal data is utilised
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: ______________________ Agreement End Date: ______________________
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement 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 Agreement. (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 District, or a successor contractor at the District'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 District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District'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: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

Contractor: **Powtoon Ltd**

Signature: ______________________________ **Date: 11-JUN-2025**

Printed Name: FEMI ONANUGA **Title: DEPUTY CISO**

EXHIBIT "C"
Contractor's Data Security & Privacy Plan

1 ORGANIZATIONAL SECURITY MEASURES

1.1 SECURITY MANAGEMENT

(a) Security policy and procedures: The data processor has a documented security policy with regard to the processing of personal data.

(b) Roles and responsibilities :

(1) Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.

(2) During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

(c) Access Control Policy: Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

(d) Resource/asset management: The data processor has a register of the IT resources used for the processing of personal data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

(e) Change management: The data processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place**.**

1.2 INCIDENT RESPONSE AND BUSINESS CONTINUITY

(a) Incidents handling / Personal data breaches:

(1) An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining personal data.

(2) The data processor will report without undue delay to the controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

(b) Business continuity: The data processor has established the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

1.3 Human resources

(a) Confidentiality of personnel: The data processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

(b) Training: The data processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2 Technical security measures

2.1 Access control and authentication

(a) An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing, and deleting user accounts.

(b) The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

(c) When granting access or assigning user roles, the "need-to-know principle" shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor's processing purposes.

(d) Where authentication mechanisms are based on passwords, the data processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

(e) The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

2.2 Logging and monitoring:

Log files are activated for each system/application used for the processing of personal data. They include all types of access to data (view, modification, deletion).

2.3 Security of data at rest

(a) Server/Database security

(1) Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.

(2) Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.

(b) Workstation security:

(1) Users are not able to deactivate or bypass security settings.

(2) Anti-virus applications and detection signatures is configured on a regular basis.

(3) Users don't have privileges to install or deactivate unauthorized software applications.

(4) The system has session time-outs when the user has not been active for a certain time period.

(5) Critical security updates released by the operating system developer is installed regularly.

2.4 NETWORK/COMMUNICATION SECURITY:

(a) Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

(b) Traffic to and from the IT system is monitored and controlled through firewalls and intrusion detection systems.

2.5 BACK-UPS:

(a) Backup and data restore procedures are defined, documented, and clearly linked to roles and responsibilities.

(b) Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

(c) Execution of backups is monitored to ensure completeness.

2.6 MOBILE/PORTABLE DEVICES:

(a) Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

(b) Mobile devices that are allowed to access the information system are pre-registered and pre-authorized.

2.7 Application lifecycle security

During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards are followed.

2.8 Data deletion/disposal:

(a) Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction will be performed.

(b) Shredding of paper and portable media used to store personal data is carried out.

2.9 Physical security:

The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures (e.g. intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g. security guard) shall be set in place to protect security areas and their access points against entry by unauthorized persons.