DATA PRIVACY AGREEMENT

Medina Central School District

And

Sophos Limited

This Data Privacy Agreement ("DPA") is by and between the Medina Central School District of 1 Mustang Drive, Medina NY 14103, U.S.A. ("EA"), an Educational Agency, and Sophos Limited of The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK ("Contractor"), collectively, the “Parties”.

RECITALS

WHEREAS, the Contractor has agreed to provide the EA with certain services ("Services") pursuant to a contract dated 7/1/2021 and expires on 6/30/2022 ("Service Agreement"); and

WHEREAS, in order to provide the Services, the Contractor may receive from the EA and the EA may provide the Contractor with PII regulated by several New York and federal laws and regulations, among them, the Federal Educational and Privacy rights Act ("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); the Individuals with Disabilities Education Act (“IDEA”) at 20 U.S.C. 1400 et seq. (34 CFR Part 300); Education Law § 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the laws referred to above.

NOW THEREFORE, the Parties agree as follows:

ARTICLE I: DEFINITIONS

As used in this agreement, the following terms shall have the following meanings:

1. **Authorized Users:** Contractor's employees and non-employee recipients.
2. **Breach:** The unauthorized acquisition, access, use, or disclosure of PII by or to a person not authorized to acquire, access, use, or receive it.
3. **Commercial or Marketing Purpose:** The sale of student data, teacher or principal data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve or market products or services to students.
4. **Contract, agreement or written agreement**: A binding agreement between an EA and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
5. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
6. **Education Record:** An education record as defined in FERPA and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
7. **Educational Agency**: A school district, board of cooperative educational services, school, charter school or the New York State Education Department.
8. **Eligible Student:** A student eighteen years or older.
9. **Encrypt or Encryption**: Methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached, as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304.
10. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://www.nist.gov/cyberframework/new-framework
11. **Parent:** A parent, legal guardian or person in parental relation to the student.
12. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family

Educational Rights and Privacy Act, 20 U.S.C. 1232g, and shall be comprised of Student Data and Teacher or Principal APPR Data, as defined below.

13. **Release:** Shall have the same meaning as Disclose.
14. **Student:** Any person attending or seeking to enroll in an Educational Agency.
15. **Student Data:** Personally Identifiable Information regarding students from the student records of an educational agency.
16. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
17. **Teacher or Principal Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews ("APPR") of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: DATA PROTECTION

1. **Purpose.** Contractor is permitted to have access to PII solely and exclusively for the purpose set forth in the Service Agreement as outlined in Exhibit B, the parents' bill of rights for data privacy and security supplemental information. Contractor agrees to hold the PII in strict confidence, and not to disclose it for the benefit of another or for any use or purpose other than for providing the Services. The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or it sub-contractors retain PII or retain access to PII.
2. **Ownership of PII**. Contractor has no property or licensing rights or claims of ownership to any PII.
3. **Right to Review.** The EA has the right to review Contractor's procedures, practices and controls related to the protection of PII. To that end, upon request, Contractor will make available for review policies, procedures, practices and documentation related to the protection of PII. The Contractor represents that it is regularly audited against SSAE 18 SOC 2 standards by independent third-party auditors. Upon written request, the Contractor shall supply a copy of its SOC 2 audit report to the EA, which reports shall be subject to the confidentiality provisions of the Agreement (or as the Contractor may reasonably request) as the Contractor's confidential information. The EA acknowledges and agrees that the third-party auditor that authored such report ("Author") does not accept any responsibility or liability to the EA or the EA's auditors unless and until the EA enters into a separate duty of care agreement with the Author. The Contractor shall also respond to any written audit questions submitted to it by the EA, provided that the EA shall not exercise this right more than once per year.

4. **Parent and Eligible Student Access**. Education Law §2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for the Contractor to facilitate such review by a Parent or Eligible Student, and as applicable, facilitate corrections as necessary other than where (i) the EA is able to view or correct the Eligible Student's Student Data themselves, or (ii) the Contractor is unable to revise, edit or correct an Eligible Student's Student Data in an Eligible Student's records held by the Contractor in which case the Contractor may decline such request. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.
5. **Compliance with Law**. Contractor agrees to maintain the confidentiality of PII in accordance with those portions of applicable New York and federal laws, rules, and regulations.
6. **Bill of Rights for Data Privacy and Security**. As required by §2-d of the Education Law, the parents bill of rights for data privacy and security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and sign Exhibit A. Pursuant to Education Law §2-d, the EA is required to post the completed Exhibit B on its website.
7. **Contractor's Authorized Users**. Contractor shall only disclose PII to Authorized Users who need to know and/or have access in order to carry out the Services, provided that such disclosure shall be made only to the extent justifiable by such need, and shall adopt and maintain administrative, physical and technical security and privacy controls and protocols that ensure access only to Authorized Users. Contractor shall ensure that all such Authorized Users comply with similar terms aligned to this DPA. Contractor agrees that upon request by the EA, it will provide the EA with the names and affiliations of the Non-Employee Recipients to whom it proposes to disclose, or has disclosed, PII. Contractor shall ensure that each Authorized User is contractually bound by an agreement that includes adequate confidentiality and data security obligations.
8. **Subcontractor.** Where a subcontractor is used by the Contractor, they shall enter into a written agreement with such subcontractor. Such written agreements shall include provisions that ensure that the subcontractors will abide by all applicable data protection and security requirements, including but not limited to those outlined in state and federal laws and regulations. Contractor shall take full responsibility for the acts and omissions of its subcontractors. Contractor shall examine the data security and privacy measures of its subcontractors before it agrees to utilize the subcontractor and shall periodically do so for as long as the subcontractor is being utilized to fulfill the Contractor's responsibilities under the

Service Agreement. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

9. **Destruction of Data**. Nothing in the Service Agreement shall authorize Contractor to maintain PII after a reasonable time following the termination of the Service Agreement. Contractor shall provide the EA a written certification of the secure deletion and/or destruction of PII held by the Contractor and its Authorized Users within a reasonable time period as agreed to by the Parties after the Service Agreement terminates. Contractor shall thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Authorized Users, securely delete and/or destroy such PII in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, and direct its Authorized Users to do the same. Contractor shall ensure that no copy, summary or extract of the PII is retained on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever by Contractor or its Authorized Users. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise cannot be reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Redaction is specifically excluded as a means of data destruction.
10. **No Sale or Commercial Use**. Contractor agrees that it will not sell PII; use or disclose PII for purposes of receiving remuneration, whether directly or indirectly; use or disclose PII for marketing, commercial or advertising purposes or facilitate its use or disclosure by any other party for such purposes; or use or disclose PII to develop, improve or market products or services to students, or permit another party to do so.
11. **Disclosure Limitations.** Unless as permitted by this DPA, Contractor shall not disclose any PII to any party who is not an Authorized User. Notwithstanding the foregoing, Contractor may disclose PII if such disclosure is required by statute or court order and the Contractor makes a reasonable effort to notify the EA of the order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by statute or court order.
12. **Encryption.** Contractor shall use industry best practices to preserve and protect PII from unauthorized disclosure. Contractor shall use Encryption technologies to protect PII at rest, on file storage, database storage, or on back-up media, and in transit/motion.
13. **Data Security and Privacy Plan**. As to the PII provided to the Contractor to meets its obligations to the EA under the Service Agreement, Contractor shall maintain reasonable administrative, technical and physical safeguards that meet New York State law and regulations, its own requirements, and generally recognized industry standards and practices, in particular alignment with the NIST Cybersecurity Framework, to protect the security, confidentiality and integrity of PII in its custody. Contractor is required to have a Data Security and Privacy Plan

that complies with 8 NYCRR Part 121 and is acceptable to the EA. Contractor's Data Security and Privacy Plan is outlined and attached to this DPA as Exhibit C.

14. **Training**. Contactor shall ensure that all Authorized Users and Subcontractors who have access to PII of the EA under the terms of the Service Agreement have received or will receive training on the confidentiality of such PII under the General Data Protection Regulation (GDPR) and understand the relevant privacy and data security obligations relating to such access. The Contractor represents that many of the chapters, general provisions, and principles of the GDPR align with the data security requirements of Education Law § 2-d and 8 NYCRR Part 121.
15. **Data Breach Reporting**. Contractor shall without undue delay notify the EA of any breach of security resulting in an unauthorized release or disclosure of PII by Contractor or its Authorized Users in violation of applicable state or federal law and/or this DPA in the most expedient way reasonably possible, but not more than seven (7) calendar days after discovery of such breach. Notification shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery, if known; a description of the types of PII affected, an estimate of the number of records affected, a brief description of the Contractor's investigation or plan to investigate, and contact information for representatives who can assist the EA.
16. **Cooperation with Investigations.** Contractor agrees that it will reasonably cooperate with the EA and law enforcement, where necessary, to protect the integrity of any investigations into a breach or unauthorized release of PII. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor.
17. **Notification Costs.** Where a breach or unauthorized release of PII occurs that is attributable to Contractor or any of its Authorized Users, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to parents, students, teachers, and/or principals, in accordance Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: MISCELLANEOUS

1. **Priority of Agreements and Precedence.** In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein, the Service Agreement, and any of Contractor's terms of service or privacy notices that apply to the Services, the terms and conditions of this DPA shall prevail. In addition, this DPA and all its Exhibits shall be deemed a part of and incorporated into the Service Agreement but shall survive the termination of the Service Agreement in the manner set forth herein.

2. **Entire Agreement**. This DPA constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.
3. **Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of New York, without regard to conflicts of law principles. The state and federal courts located in New York will have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this DPA, the Service Agreement referenced in this DPA, or the transactions contemplated hereby.
4. **Execution.** This DPA as well as attached Exhibits A and B may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document. This DPA as well as the attached exhibits A and B may be executed by electronic transmittal documents in lieu of an original or machine generated or copied document, and each signature thereto shall be and constitute an original signature, as if all Parties had executed a single original document.
5. **Liability.** In no event shall the Contractor's liability in connection with any issue arising out of, or in connection with, this DPA exceed the Contractor's limitations on liability set out in the Service Agreement. The Contractor's limitations on liability as set out in the Service Agreement shall apply in aggregate across both the Service Agreement and this DPA, such that a single limitation on liability regime shall apply across both the Service Agreement and this DPA.

SOPHOS LIMITED

Signature: sbd fillingham
sbd fillingham (Jul 21, 2021 15:11 GMT+1)

Printed Name: sbd fillingham

Title/Position: Director

Date: Jul 21, 2021

MEDINA CENTRAL SCHOOL DISTRICT

Signature: Anthony Moreno
Anthony Moreno (Jul 29, 2021 10:29 EDT)

Printed Name: Anthony Moreno

Title/Position: Data Protection Officer

Date: Jul 29, 2021

EXHIBIT A - EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Medina Central 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 at www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5) Parents have the right to 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 www.nysed.gov/data-privacy-security/report-improper-disclosure

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Medina Central 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.

SOPHOS LIMITED

Signature: sbd fillingham
sbd fillingham (Jul 21, 2021 15:11 GMT+1)

Printed Name: sbd fillingham

Title/Position: Director

Date: Jul 21, 2021

EXHIBIT B - BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

The Educational Agency is required to post information to its website about its agreements with third-party contractors that will receive PII pursuant to Education Law §2-d and Part 121.3 of the Commissioner's Regulations.

Contact information for notifications of any breach of security resulting in an unauthorized release or disclosure of PII by Contractor or its Authorized Users is as follows:

Medina CSD Data Protection Officer (DPO):

- Name: Anthony Moreno
- Email: amoreno@medinacsd.org
- Phone: 585-798-1534
- Address: 1 Mustang Drive, Medina NY 14103

Name of Vendor	Sophos Limited
Products	Phish Threat and Device Encryption
Description of Services	N/A
Type of PII that Contractor will receive/access	_X_ Student Data __ APPR Data
Service Agreement Term (Start and End Dates)	July 1, 2021 – June 30, 2022
Subcontractors	__X__ Contractor will utilize subcontractors in accordance with the terms of the DPA and shall require, pursuant to written agreement, that its subcontractors adhere to appropriate data protection obligations. _____ Contractor will not utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Service Agreement, Contractor shall: ✓ Securely transfer data to EA, in a format agreed to by the parties; ✓ Securely delete and destroy the PII; and, ✓ Certify to EA that secure deletion is complete.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII may do so by contacting the EA's Data Protection Officer, who will review all such requests. If a correction to PII is deemed necessary, Contractor will work with the EA to make such corrections, as applicable.
Secure Storage and Data Security	Please describe where PII will be stored and the protections take to ensure PII will be protected (check all that apply): _X__ 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: Sophos maintains an Information Security Management System which comprises risk based security controls which are managed and monitored by a dedicated security function and security tools and processes. The Sophos ISMS comprises personnel controls, physical security, access management, data security, asset management, secure development, security monitoring and incident response.
Encryption	_X__ PII will be encrypted while in motion and at rest.

SOPHOS LIMITED

Signature: sbd fillingham
sbd fillingham (Jul 21, 2021 15:11 GMT+1)

Printed Name: sbd fillingham

Title/Position: Director

Date: Jul 21, 2021

EXHIBIT C - 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 and/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 requirements over the life of the Service Agreement.	Sophos maintains an Information Security Management System which comprises risk based security controls which are managed and monitored by a dedicated security function and security tools and processes.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	The Sophos ISMS comprises personnel controls, physical security, access management, data security, asset management, secure development, security monitoring and incident response.
3	Certify compliance with the requirements set forth in the Supplemental Information to the Parents Bill of Rights.	Sophos is certified to SOC2. Audits are underway for a number of certifications, including to ISO27001.
4	Specify how Authorized Users have been trained or will receive training on recognized standards governing confidentiality of such data prior to receiving access.	Authorized User Training relates to that required under the provisions of the EU General Data Protection Regulation (GDPR). For the purposes of complying with its obligations under the Service Agreement and DPA with the EA, the Contractor represents that many of the chapters, general provisions, and principles of the GDPR align with the data security requirements of Education Law § 2-d and 8 NYCRR Part 121.
5	Outline contracting process that ensures that Authorized users are bound by confidentiality obligations to the requirements of this DPA, at a minimum.	The Sophos vendor risk assessment process ensures that data protection requirements are in place.

6	Specify how you will manage any data security and privacy incidents that involve PII and describe any specific plans you have in place to identify data breaches and unauthorized disclosures, and to meet your obligations to report incidents to the Educational Agency.	The Sophos Cybersecurity team runs an incident response process, which comprises detection, analysis, containment, eradication and recovery. Relevant incidents are escalated to the data protection team to ensure any notification requirements are met.
7	Describe how PII will be transitioned to the Educational Agency when no longer needed by Contractor to provide Services, if applicable.	Sophos should not be in possession of any data not already held by the Educational Agency. However, should data transfer be required this will be carried out using a secure, encrypted connection, as agreed with the recipient.
8	Describe secure destruction practices and how certification will be provided to the Educational Agency.	Secure destruction is typically carried out by contracted third parties, who provide confirmation of the deletion. This certification will be provided to the Education Agency as applicable.