

**NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT
VERSION (2019)**

Prospect Mountain School District

and

Sophos Limited

August 3, 2020

This New Hampshire Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Prospect Mountain School District (hereinafter referred to as “LEA”) and Sophos Limited (hereinafter referred to as “Provider”) on August 3, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the LEA with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the services described in Article 1 and Appendix A (“Services”), the Provider may receive and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from New Hampshire LEAs to the Provider for the provision of the Services are also subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

- 1** **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data and Teacher Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) and Teacher Data are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate institutional interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA with respect to the use and maintenance of Student Data and Teacher Data.

- 2** **Nature of Services Provided.** The Provider has agreed to provide the services described in Exhibit “A”.

- 3 **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of Student Data and Teacher Data described in the Schedule of Data, attached hereto as Exhibit “B”.
- 4 **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1 **Student Data Property of LEA.** All Student Data, Teacher Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data, Teacher Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data, Teacher Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data, Teacher Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data and Teacher Data notwithstanding the above. The LEA will have access and be able to download at any time Student Data and Teacher Data. Provider may transfer Pupil Generated Content to a separate account, according to the procedures set forth below.
- 2 **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. The LEA will be able to revise, correct or modify Student or Teacher Data at any time. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records or Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
- 3 **Separate Account.** Provider shall, at the request of the LEA, transfer Pupil Generated Content to the LEA.
- 4 **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data or Teacher Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and

shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data, Teacher Data, and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data, Teacher Data, and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data and Teacher Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

- 5 **No Unauthorized Use.** Provider shall not use Student Data, Teacher Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

- 6 **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data and Teacher Data in manner similar to the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data and Teacher Data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.

2. **Authorized Use.** Student Data and Teacher Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this

DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that, other than to affiliates or sub-processors, it shall not make any re-disclosure of any Student Data, Teacher Data, or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data or Teacher Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data or Teacher Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality obligation from each employee or agent with access to Student Data or Teacher Data pursuant to the DPA.

4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and Teacher Data and not to transfer de-identified Student Data and Teacher Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which de-identified data is presented

5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable Student Data and Teacher Data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA’s designee within one hundred and twenty (120) days of the date of receipt by the Provider of a reasonable written request to do so by the LEA and according to a schedule and procedure as the Parties may reasonably agree in writing. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition unless required by law to do so. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Student Data and Teacher Data has been disposed. The duty to dispose of Student Data and Teacher Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” FORM, A Copy of which is attached hereto as Exhibit “D”).

6. **Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data or Teacher Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data and Teacher Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data and Teacher Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data and Teacher Data to employees or contractors that are performing the Services. If any student contacted Provider, Provider will redirect them to the LEA.
 - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and Teacher Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to a schedule and procedure as the parties may reasonable agree in writing. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition unless required by law to do so.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data or Teacher Data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data and Teacher Data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit Student Data and Teacher Data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers or sub-processors to view or access data as set forth in Article IV, section 4.
 - d. **Employee Training.** The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider’s business and cover,

but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

- e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer (“SSL”), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
- f. The LEA may contact the Provider’s IT Security Team by email at: DataProtection@Sophos.com.
- g. LEFT BLANK
- h. LEFT BLANK
- i. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- j. **Audits** The Provider will, at the cost of the LEA for Provider’s work beyond gathering existing documents and information at the hourly rate of the applicable employees, cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any federal/state audit or investigation of the LEA and/or delivery of Services to students and/or LEA. The LEA acknowledges that the Provider is regularly audited against SSAE 18 SOC 2 standards by independent third-party auditors. Upon request, the Provider shall supply a copy of its SOC 2 audit report to the LEA, which reports shall be subject to the confidentiality provisions of the Agreement as the Provider’s confidential information. The LEA acknowledges and agrees that the third-party auditor that authored such report (“**Author**”) does not accept any responsibility or liability to the LEA or the LEA’s auditors unless and until the LEA enters into a separate duty of care agreement with the Author. The Provider shall also respond to any written audit questions submitted to it by the LEA, provided that the LEA shall not exercise this right more than once per year.
- k. **New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from “the Minimum Standards for Privacy and Security of Student and Employee Data” from the New Hampshire Department of Education. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;

- (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
- (4) Authorize wireless access prior to allowing such connections;
- (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
- (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
- (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
- (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

Enforce a minimum password complexity and change of characters when new passwords are created;

- (9) Perform maintenance on organizational systems;
- (10) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- (11) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
- (12) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
- (13) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- (14) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
- (15) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- (16) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

- (17) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (18) Protect the confidentiality of Student Data and Teacher Data at rest;
- (19) Identify, report, and correct system flaws in a timely manner;
- (20) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (21) Monitor system security alerts and advisories and take action in response; and
- (22) Update malicious code protection mechanisms when new releases are available.

2 Data Breach. Upon confirming the occurrence of a Data Breach, the Provider shall inform the LEA within thirty days and shall provide all such timely information and cooperation as the LEA may reasonably require in order for the LEA to fulfil its Data Breach reporting obligations. The Provider shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Data Breach and shall keep the LEA informed of all developments in connection with the data breach. Any notification by the Provider to the LEA of any confirmed Data Breach pursuant to this clause will be made by email to the email address specified by the LEA to the Provider in this DPA.

- a.** The Data Breach notification described above shall include, at a minimum, the following information:
 - i.** A list of the types of personal information that were or are reasonably believed to have been the subject of a Data Breach.
 - ii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the Data Breach, (2) the estimated date of the Data Breach, or (3) the date range within which the Data Breach occurred. The notification shall also include the date of the notice.
 - iii.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - iv.** A general description of the Data Breach incident, if that information is possible to determine at the time the notice is provided.
 - v.** The estimated number of students and teachers affected by the Data Breach, if any.
- b.** At LEA's discretion, the Data Breach notification may also include any of the following:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.

- ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- c. Provider agrees to adhere to all requirements in the New Hampshire Data Breach law and in federal law with respect to a Data Breach related to the Student Data and Teacher Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Data Breach.
- d. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Data Breach and agrees to make staff available at reasonable times to answer questions of the LEA on the written incident response plan..

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data or Teacher Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years or until the termination of a Service Agreement, whichever occurs first.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service of the Provider (“EULA”) , to the extent one exists, has (i) lapsed, or (ii) has been terminated in accordance with clause 12 of the EULA.

The LEA may terminate this DPA and the EULA as set out in the EULA if the Provider breaches the terms of this DPA and the LEA shall be entitled to receive a pro rata refund of any prepaid fees for the period remaining after such termination.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA’s data pursuant to Article V, section 1(b).
4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA, COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.
5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid,

sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

Name	Data Privacy Team
Title	_____
Address	The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP
Telephone Number	_____
Email	DataProtection@Sophos.com

The designated representative for the LEA for this Agreement is:

Tom Rubino IT Director/Information Security Officer
trubino@pmhschool.com 603-875-3800 x3205
Prospect Mountain High School
242 Suncook Valley Road, Alton, NH 03809

- 6. 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. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
- 7. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 8. Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF BELKNAP COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data, Teacher Data, and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data, Teacher Data, and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data, Teacher Data, and any portion thereof is stored, maintained or used in any way.
10. **Waiver.** No delay or omission of either party to exercise any right hereunder shall be construed as a waiver of any such right and such party reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This DPA may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this DPA. In proving this DPA, it shall not be necessary to produce or account for more than one such counterpart.

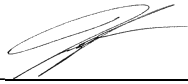
ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (“General Offer”, attached hereto as Exhibit “E”), be bound by the terms of this to any other New Hampshire school district who signs the acceptance in said Exhibit.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this New Hampshire Student Data Privacy Agreement as of the last day noted below.

PROSPECT MOUNTAIN SCHOOL DISTRICT

By:  _____ Date: 1-28-21

Printed Name: Tom Rubino Title/Position: IT Director

SOPHOS LIMITED

By: *sbd fillingham* _____ Date: Jan 27, 2021
sbd fillingham (Jan 27, 2021 11:53 GMT)

Printed Name: sbd fillingham Title/Position: Director

EXHIBIT “A”

DESCRIPTION OF SERVICES

Sophos Intercept X employs a comprehensive defense-in-depth approach to endpoint protection, rather than simply relying on one primary security technique. This is the “the power of the plus” – a combination of leading foundational and modern techniques. Modern techniques include deep learning malware detection, exploit prevention, and anti-ransomware specific features. Foundational techniques include signature-based malware detection, behavior analysis, malicious traffic detection, device control, application control, web filtering, data loss prevention, and more.

EXHIBIT “B”

SCHEDULE OF STUDENT DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	Yes
	Other application technology meta data-Please specify:	See note below.
Application Use Statistics	Meta data on user interaction with application	Yes
Assessment	Standardized test scores	No
	Observation data	No
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	No
	Student class attendance data	No
Communications	Online communications that are captured (emails, blog entries)	No
Conduct	Conduct or behavioral data	No
Demographics	Date of Birth	No
	Place of Birth	No
	Gender	No
	Ethnicity or race	No
	Language information (native, preferred or primary language spoken by student)	No
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	No
	Student grade level	No
	Homeroom	No
	Guidance counselor	No
	Specific curriculum programs	No
	Year of graduation	No
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	No
	Email	No
	Phone	No
Parent/Guardian ID	Parent ID number (created to link parents to students)	No
Parent/Guardian Name	First and/or Last	No

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	No
	Teacher names	No
Special Indicator	English language learner information	No
	Low income status	No
	Medical alerts	No
	Student disability information	No
	Specialized education services (IEP or 504)	No
	Living situations (homeless/foster care)	No
	Other indicator information-Please specify:	No
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	No
	Email	No
	Phone	No
Student Identifiers	Local (School district) ID number	No
	State ID number	No
	Vendor/App assigned student ID number	No
	Student app username	No
	Student app passwords	No
Student Name	First and/or Last	No
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	No
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	No
Student Survey Responses	Student responses to surveys or questionnaires	No
Student work	Student generated content; writing, pictures etc.	No
	Other student work data - Please specify:	No
Transcript	Student course grades	No
	Student course data	No

Category of Data	Elements	Check if used by your system
	Student bus card ID number	No
	Other transportation data - Please specify:	No
Other	Please list each additional data element used, stored or collected by your application	See note below.

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	No
	Other transcript data -Please specify:	No
Transportation	Student bus assignment	No
	Student pick up and/or drop off location	No

SCHEDULE OF TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	Yes
	Other application technology meta data-Please specify:	See note below.
Application Use Statistics	Meta data on user interaction with application	Yes
Communications	Online communications that are captured (emails, blog entries)	No
Demographics	Date of Birth	No
	Place of Birth	No
	Social Security Number	No
	Ethnicity or race	No
	Other demographic information-Please specify:	N/A

Personal Contact Information	Personal Address	No
	Personal Email	No
	Personal Phone	No
Performance evaluations	Performance Evaluation Information	No
Schedule	Teacher scheduled courses	No
Special Information	Medical alerts	No
	Teacher disability information	No
	Other indicator information- Please specify:	N/A
Teacher Identifiers	Local (School district) ID number	No
	State ID number	No
	Vendor/App assigned student ID number	No

Category of Data	Elements	Check if used by your system
	Teacher app username	No
	Teacher app passwords	No
Teacher In App Performance	Program/application performance	No
Teacher Survey Responses	Teacher responses to surveys or questionnaires	No
Teacher work	Teacher generated content; writing, pictures etc.	No
	Other teacher work data - Please specify:	No
Education	Course grades from schooling	No
	Other transcript data -Please specify:	N/A
Other	Please list each additional data element used, stored or collected by your application	See note below.

Note:

Specific to Sophos Central, the following PII is collected –

1. Sophos Central administrator login information - emails and passwords
2. User data both manually and automatically entered via Active Directory Synchronization - username, login, Exchange login, AD group information
3. Policy information - settings (dependent of policy components), or example exemptions
4. Device information - device name, last user, operating system information, status
5. Events – type, e.g., web, device, malware, device information (file and path names, network locations, logins, etc.)
6. Sophos Central does not store all end-users' browsing history; only web events for "blocked" and "warned" pages are retained for reporting purposes.

EXHIBIT “C”

DEFINITIONS

Data Breach: An unauthorized acquisition of Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records or Teacher Data in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, Student Data, Teacher Data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

- | | |
|---|-----------------------------|
| First Name | Home Address |
| Last Name | Subject |
| Telephone Number | Email Address |
| Discipline Records | Test Results |
| Special Education Data | Juvenile Dependency Records |
| Grades | Evaluations |
| Criminal Records | Medical Records |
| Health Records | Social Security Number |
| Biometric Information | Disabilities |
| Socioeconomic Information | Food Purchases |
| Political Affiliations | Religious Information |
| Text Messages | Documents |
| Student Identifiers | Search Activity |
| Photos | Voice Recordings |
| Videos | Date of Birth |
| Grade | Classes |
| Place of birth | Social Media Address |
| Unique pupil identifier | |
| Credit card account number, insurance account number, and financial services account number | |
| Name of the student's parents or other family members | |

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email

Provider: For purposes of the DPA, the term “Provider” means provider of digital services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

Student Data: Student Data includes any data, provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, the name of the student’s parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of New Hampshire and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services.

Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software and the Services, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or Pupil Generated Content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Teacher: It includes teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

Teacher Data: For the purposes of this DPA, it applies to teachers, paraprofessionals, principals, school employees, contractors, and other administrators. It includes at least the following:

Social security number.

Date of birth.

Personal street address.

Personal email address.

Personal telephone number

Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs SOPHOS LIMITED to dispose of data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

___ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

___ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

___ As soon as commercially practicable

___ By (Insert Date)

4. Signature

(Authorized Representative of LEA)

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

OPTIONAL: EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? Yes No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a Data Breach? If so which one(s):

_____ ISO 27001/27002

_____ CIS Critical Security Controls

_____ NIST Framework for Improving Critical Infrastructure Security

_____ Other: _____

3. Does your organization store any customer data outside the United States? Yes No

4. Does your organization encrypt customer data both in transit and at rest? Yes No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Ross McKerchar

Contact information: Email address: Ross.McKerchar@sophos.com

6. Please provide any additional information that you desire.






Sophos_ProspectMountain

Final Audit Report

2021-01-28

Created:	2021-01-28
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAPtupi68jQYunnbWl617ndsHQzV0SvGav

"Sophos_ProspectMountain" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2021-01-28 - 1:54:14 PM GMT- IP address: 100.1.115.187
-  Document emailed to Tom Rubino (trubino@pmhschool.com) for signature
2021-01-28 - 1:55:05 PM GMT
-  Email viewed by Tom Rubino (trubino@pmhschool.com)
2021-01-28 - 1:56:02 PM GMT- IP address: 66.102.8.19
-  Document e-signed by Tom Rubino (trubino@pmhschool.com)
Signature Date: 2021-01-28 - 2:38:59 PM GMT - Time Source: server- IP address: 184.61.100.22
-  Agreement completed.
2021-01-28 - 2:38:59 PM GMT