SOPHOS
Cybersecurity made simple.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is entered into between **Sophos Limited**, a company registered in England and Wales number 2096520, with its registered office at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK ("**Supplier**"), and the following party ("**Customer**"):

Customer: Newfane Central School District

1. PREAMBLE

The parties have entered into one or more of the following agreements: (1) if the Customer is an end user ("**End User**"), an end user license agreement, located at https://www.sophos.com/legal.aspx ("**EULA**"), (2) if the Customer is a managed service provider ("**MSP**"), an MSP agreement located at https://www.sophos.com/en-us/legal/sophos-msp-partner-terms-and-conditions.aspx ("**MSP Agreement**"), (3) if the Customer is an End User, a professional services agreement located at https://www.sophos.com/en-us/legal/sophos-professional-services.aspx ("**Professional Services Agreement**"); in each case regarding the provision by the Supplier to the Customer of certain Hosted Products and/or other products (collectively, "**Products**"), and/or related maintenance and technical support services for such Products, and/or professional services (the "**Services**") purchased by the Customer.

The provision of the Products and Services may include the collection, processing and use of Controller Data by the Supplier for the Customer. This Agreement sets forth the obligations of the parties with respect to such data processing and supplements the terms and conditions of the Main Agreement.

The Main Agreement, this Agreement and the documents expressly referenced in the Main Agreement and this Agreement shall constitute the entire agreement between the parties in relation to Personal Data collected, processed and used by the Supplier on behalf of the Customer, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

2. DEFINITIONS

2.1 In this Agreement, the following terms shall have the following meanings:

"**Applicable Data Protection Laws**" means (i) EU Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"); (ii) the e-Privacy Directive (EU Directive 2002/58/EC); and (iii) any and all applicable national data protection legislation, including legislation made under or pursuant to (i) or (ii); in each case as may be amended or superseded from time to time.

"**Beneficiary**" has the meaning given to it in the MSP Agreement.

"**Controller**" means either: (a) the Customer, if the Customer is an End User; or (b) the Beneficiary, if the Customer is a MSP.

"**Controller Data**" means any and all personal data for which the Controller is the controller under Applicable Data Protection Laws.

"**Europe**" (and "**European**") means (i) the Member States of the European Economic Area, and (ii) with immediate effect following its withdrawal from the European Union, the United Kingdom.

"**Hosted Products**" mean the products listed in **Exhibit 3**.

"**Main Agreement**" means the EULA, MSP Agreement, and/or Professional Services Agreement (whichever the parties have entered into).

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Data processed by the Supplier under this Agreement.

2.2 In this Agreement, the lower case terms "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law.

3. SCOPE

3.1 The subject matter and duration of the Supplier's processing of Controller Data, including the nature and purpose of the processing, the types of Controller Data to be processed, and the categories of data subjects, shall be as described in: (i) this Agreement; (ii) the Main Agreement; (iii) the privacy policy at https://www.sophos.com/en-us/legal/sophos-group-privacy-policy.aspx, including the Product Privacy Information page at https://www.sophos.com/en-us/legal/product-privacy-info.aspx ("**Sophos Privacy Policy**"); (iv) any instructions in **Exhibit 1**; and (v) the Customer's instructions issued in accordance with Clause 4.

3.2 The Customer is responsible for ensuring (i) that the Controller has a lawful basis for the processing of Controller Data that will be carried out by the Supplier on its behalf, and (ii) that the Controller has obtained all necessary consents from data subjects that may be required for the processing of Controller Data by the Customer and the Supplier (including but without limitation, in relation to special categories of data); and (iii) that it is otherwise compliant with, and will ensure its instructions to the Supplier for the processing of Controller Data comply in all respects with, Applicable Data Protection Laws.

3.3 The remaining provisions of this Agreement describe the parties' respective obligations in relation to Controller Data for which either: (i) the Customer is the controller and the Supplier is the processor, if the Customer is an End User; or (ii) the Customer is the processor for a third party Controller, and the Supplier is the sub-processor, if the Customer is a MSP.

3.4 If multiple Main Agreements exist between the parties, then a separate instance of this Agreement shall apply with respect to each Main Agreement.

4. CUSTOMER INSTRUCTIONS

4.1 The Supplier shall process the Controller Data in accordance with the Customer's documented processing instructions, as exclusively set out in Clause 3.1 except:

(a) where otherwise agreed in writing between the Supplier and the Customer; or

(b) where required by European law to which the Supplier is subject (in which event, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits the provision of such information).

4.2 If the Supplier becomes aware that the Customer's processing instructions infringe Applicable Data Protection Laws (without imposing any obligation on the Supplier to actively monitor the Customer's compliance), it will promptly notify the Customer of same and suspend processing of the Controller Data.

5. DUTIES OF THE SUPPLIER

5.1 All Supplier personnel who process the Controller Data shall be adequately trained with respect to their data protection, security and confidentiality obligations, and shall be subject to written obligations to maintain confidentiality.

5.2 The Supplier will, at its own cost, implement appropriate technical and organisational measures to protect the Controller Data against a Personal Data Breach. Such measures will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons so as to ensure a level of security that is appropriate to the risk. In particular, the measures taken by the Supplier shall include those described in **Exhibit 2** of this Agreement. The Supplier may change or amend the technical and organisational measures described in **Exhibit 2** without the prior written consent of the Customer provided that the Supplier maintains at least an equivalent level of protection. Upon request by the Customer, the Supplier will provide an updated description of the technical and organisational measures in the form as presented in **Exhibit 2**.

5.3 The Supplier shall follow the requirements specified in Clause 7 for engaging any subprocessor to process Controller Data.

5.4 The Supplier shall follow the requirements specified in Clause 8 for assisting the Customer to respond to enquiries from third parties, including any requests from data subjects to exercise their rights under Applicable Data Protection Laws.

5.5 Upon confirming the occurrence of any Personal Data Breach, the Supplier shall inform the Customer without undue delay and shall provide all such timely information and cooperation as the Customer may reasonably require in order for the Customer (and, if the Customer is an MSP, its Controller) to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. The Supplier shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Personal Data Breach and shall keep the Customer informed of all developments in connection with the Personal Data Breach. Any notification by the Supplier to the Customer of any confirmed Personal Data Breach pursuant to this Clause will be made by email to the "Incident Reporting Email" address specified by the Customer in this Agreement.

5.6 The Supplier shall provide the Customer (or, if the Customer is an MSP, its Controller) with all such reasonable and timely assistance as the Customer (or, as applicable, the Controller) may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority. Such assistance shall be provided at the Customer's expense.

5.7 The Supplier shall delete the Controller's Controller Data within a reasonable period of time following termination or expiry of this Agreement, in each case if and to the extent permitted by applicable European law.

5.8 The Supplier shall follow the requirements specified in Clause 6 for providing to the Customer (and, if the Customer is an MSP, its Controller) such information as is necessary to demonstrate the Supplier's compliance with the obligations laid down in this Agreement.

6. AUDIT RIGHTS OF THE CUSTOMER

6.1 The Customer acknowledges that the Supplier is regularly audited against SSAE 18 SOC 2 standards by independent third party auditors. Upon request, the Supplier shall supply a copy of its SOC 2 audit report to the Customer, which reports shall be subject to the confidentiality provisions of the Main Agreement as the Supplier's confidential information. The Customer acknowledges and agrees that the third party auditor that authored such report ("**Author**") does not accept any responsibility or liability to the Customer or the Customer's auditors unless and until the Customer enters into a separate duty of care agreement with the Author. The Supplier shall also respond to any written audit questions submitted to it by the Customer, provided that the Customer shall not exercise this right more than once per year.

7. SUBPROCESSORS

7.1 The Customer consents to the Supplier's existing subprocessors as at the date of this Agreement, which are listed at https://www.sophos.com/en-us/legal ("**Subprocessor List**"). The Supplier will not subcontract the processing of any Controller Data to any additional third party subprocessors (each a "**New Subprocessor**") without the prior written consent of the Customer. The Supplier will provide prior notice of the addition of any New Subprocessor (including general details of the processing it performs or will perform), which notice may be given by posting details of such addition to the Subprocessor List. If the Customer does not object in writing to the Supplier's appointment of a New Subprocessor (on reasonable grounds relating to the protection of Controller Data) within 30 days of the Supplier adding that New Subprocessor to the Subprocessor List, the Customer agrees that it will be deemed to have consented to that New Subprocessor. If the Customer provides such a written objection to the Supplier, the Supplier will notify the Customer in writing within 30 days that either: (i) the Supplier will not use the New Subprocessor to process the Controller Data; or (ii) the Supplier is unable or unwilling to do so. If the notification in paragraph (ii) is given, the Customer may, within 30 days of such notification, elect to terminate this Agreement and the Main Agreement as to the affected processing upon written notice to the Supplier and Supplier shall for Customers located within the European Economic Area only, authorize a pro rata refund or credit of any prepaid fees for the period remaining after the termination. However, if no such notice of termination is provided within that timeframe, the Customer will be deemed to have consented to the New Subprocessor. The Supplier will impose data protection terms on New Subprocessors to protect the Controller Data to the same standard as provided for by this Agreement and the Supplier will remain fully liable for any breach of this Agreement that is caused by any such subprocessor.

8. INQUIRIES OF THIRD PARTIES

8.1 The Supplier shall provide all reasonable and timely assistance to the Customer (or, if the Customer is an MSP, the Controller), at the Customer's expense, to enable the Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Controller Data. If any such request, correspondence, enquiry or complaint is made directly to the Supplier, the Supplier shall promptly inform the Customer providing full details of the same.

9. INTERNATIONAL DATA TRANSFERS

9.1 Certain Hosted Products enable the Customer to choose whether to host the Controller Data for such products in data centres that may be located in (i) the European Economic Area, (ii) the United Kingdom, or (iii) the United States of America ("**Central Storage Location**"). This selection takes place at the point of installation. Once selected, the Central Storage Location cannot be varied at a later date.

9.2 The Customer acknowledges and agrees that, regardless of the selected Central Storage Location (if relevant), Controller Data may be exported through or to other jurisdictions (inside and/or outside of the United Kingdom and the European Economic Area): (i) to Sophos's global team of technicians and engineers for malware, security threat, and false positive analysis, and research and development purposes, (ii) in order to provide technical and customer support, account management, billing and other ancillary functions, and (iii) as expressly described in the documentation referenced in Clause 3.1.

9.3 The Supplier shall not transfer the Controller Data (nor permit the Controller Data to be processed in or from) a country outside of Europe unless it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Laws,

including, for example but without limitation, by use of the EU model clauses for controller to processor transfers.).

9.4 The transfer restriction described in Clause 9.3, shall also apply to transfers of Controller Data from the European Economic Area to the United Kingdom if and when the United Kingdom ceases to be subject to European Union law. In such event, the Supplier shall not transfer Controller Data from the European Economic Area to the United Kingdom unless it takes such measures as are necessary to ensure the transfer is in compliance with the GDPR, for example but without limitation, by use of the EU standard contractual clauses for controller to processor transfers.

9.5 If:

(a) Clause 9.3 applies because the Supplier or a Supplier affiliate will process Controller Data in a country outside of Europe; and/or

(b) Clause 9.4 applies because the Supplier or a Supplier affiliate will process Controller Data in the United Kingdom;

then in either such case, but only if and to the extent that, for any such transfers of Controller Data, no other measure recognised by the GDPR for permitting such transfers is available (such as, without limitation, transfer to a recipient in a country that the European Commission has decided provides adequate protection for personal data, transfer to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Laws, or transfer to a recipient in the United States of America that maintains a valid and up-to-date EU-US Privacy Shield certification), the parties agree that, in relation only to the Controller Data that is the subject of any such transfers where no other measure is available ("**SCCs Controller Data**"), the European Commission's 2010 standard contractual clauses for controller to processor transfers (as may be amended or superseded from time to time) ("**SCCs**") shall be incorporated into this Agreement by reference on the following basis:

i. references to the "data exporter" in the SCCs shall mean the Customer;

ii. references to the "data importer" in the SCCs shall mean Supplier and/or the relevant Supplier affiliate;

iii. the governing law specified in Clause 9 of the SCCs shall be the law of the country in which the Customer is established;

iv. Appendix 1 to the SCCs shall be deemed completed with the information that is provided in Exhibit 1 to this Agreement in relation the SCCs Controller Data; and

v. Appendix 2 to the SCCs shall be deemed completed with the information that is provided in Exhibit 2 to this Agreement.

10. DURATION

10.1 This Agreement commences upon execution by both parties and continues until the earlier of: (i) the expiry of the Customer's entitlement to use and receive the Products and Services, as noted in the Main Agreement or on any associated license entitlement; and (ii) the termination of the Main Agreement.

11. OTHER REGULATIONS

11.1 Modifications of and amendments to this Agreement require the written form. This also applies to changes and modifications to this Clause 11.1.

11.2 In no event shall the Supplier's liability to the Customer in connection with any issue arising out of, or in connection with, this Agreement exceed the Supplier's limitations on liability set out in the Main Agreement. The Supplier's limitations on liability as set out in the Main Agreement shall apply in aggregate across both the Main Agreement and this Agreement, such that a single limitation on liability regime shall apply across both the Main Agreement and this Agreement.

11.3 This Agreement shall be governed by and construed in accordance with the laws of England and Wales, without regard to conflict of laws principles. To the extent permitted by applicable law, the courts of England shall have exclusive jurisdiction to determine any dispute or claim that may arise out of, under, or in connection with this Agreement.

Signed by and on behalf of:

Newfane Central School District

Signed: Jeffrey Anstett
Jeffrey Anstett (Nov 12, 2021 10:06 EST)

Name: Jeffrey Anstett

Title: District DPO

Date: Nov 12, 2021

Incident Reporting Email:
(clause 5.5)
janstett@newfanecentralschools.org

Sophos Limited

Signed: sbd fillingham
sbd fillingham (Nov 11, 2019)

Name: Stuart Fillingham

Title: Director

Date: Nov 11, 2019

sbd fillingham
E-signed 2019-11-11 10:16AM GMT
stuart.fillingham@sophos.com

SOPHOS
Cybersecurity made simple.

Exhibit 1
Data Processing Instructions

This Exhibit 1 describes the processing that the Supplier will perform on behalf of the Customer.

This Exhibit supplements the data processing activities described in the Sophos Privacy Policy.

Subject matter, nature and purpose of the processing operations
The Controller Data will be subject to the following basic processing activities (please specify):

- Providing the Products and Services purchased by the Customer under the Main Agreement
- Providing account management and customer technical support services

The Supplier provides Products and Services that are designed to detect and prevent security threats within systems, devices, files, and other data made available by the Customer. The Supplier does not determine the content of any information held in these systems, devices, files and other data, which is determined solely by the Customer, and the Supplier processes these systems, devices, files, and other data solely for the purpose of providing the security Products and Services procured by the Customer.

Duration of the processing operations:
The Controller Data will be processed for the following duration (please specify): The duration specified in Clause 10 of the Agreement.

Data subjects
The Controller Data concern the following categories of data subjects (please specify):

Data subjects include the individuals about whom data is provided to the Supplier via the Products and Services by (or at the direction of) Customer or Customer‘s end users.

Types of personal data
The Controller Data concern the following categories of data (please specify):

Data relating to individuals provided to the Supplier via the Products and Services, by (or at the direction of) Customer or by Customer‘s end users

Special categories of data (if appropriate)
The Controller Data concern the following special categories of data (please specify):

Unless otherwise specified, the Supplier’s Products and Services are not designed to process special categories of data.

Exhibit 2
Technical and Organisational Measures

Certain of these measures may only be relevant or applicable to Hosted Products.

A) Physical Access Control.

- Sophos has a physical access control policy;
- All staff carry ID / access badges;
- Entrances to facilities are protected by access badges or keys;
- Facilities are divided into (i) public access areas (such as reception areas), (ii) general staff access areas, and (iii) restricted access areas which may only be accessed by those personnel with an express business need;
- Access badges and keys control access to restricted areas within each facility according to an individual's authorised access levels;
- Access levels for individuals are approved by senior staff members and are verified on a quarterly basis;
- Reception and/or security staff are present at entrances to larger sites;
- Facilities are protected by alarms;
- Visitors are pre-registered and visitor logs are maintained.

B) System Access Control.

- Sophos has a logical access control policy;
- The network is protected by firewalls at each Internet connection;
- The internal network is segmented by firewalls based on application sensitivity;
- IDS and other threat detection and blocking controls run on all firewalls;
- Filtering of network traffic is based on rules that apply the principle of "least access";
- Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- Passwords are strength tested and changes are enforced to weak passwords;
- Screens and sessions automatically lock after a period of inactivity;
- Sophos malware protection products are installed as standard;
- Regular vulnerability scans are conducted on IP addresses and systems;
- Systems are patched on a regular cycle with a prioritisation system for fast-tracking urgent patches.

C) Data Access Control.

- Sophos has a logical access control policy;
- Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- Passwords are strength tested and changes are enforced to weak passwords;
- Screens and sessions automatically lock after a period of inactivity;
- Laptops are encrypted using Sophos encryption products;
- Senders are directed to consider file encryption prior to sending any external email.

D) Input Control.

- Access to all systems and applications is controlled by a secure log-on procedure;
- Individuals have unique user IDs and passwords for their own use;
- The Sophos Central Products use transfer layer encryption to protect data in transit;

- Communication between the client software and the backend Sophos system is performed over HTTPS to secure the data in transit, establishing trust communication via certificates and server validation.

E) Subcontractor Control.

- Subcontractors with access to data undertake an IT security vetting procedure prior to onboarding and as required thereafter;
- Contracts contain an appropriate confidentiality and data protection obligations based on the subcontractor's duties.

F) Availability Control.

- Sophos protects its premises from fire, flood and other environmental hazards;
- Back-up generators are available to maintain power supplies in the event of power outages;
- Data centres and server rooms use climate controls and monitoring;
- The Sophos Central system is load balanced and has failover between three sites, each running two instances of the software, any one of which is capable of providing the full service.

G) Segregation Control.

- Sophos maintains and applies a quality control process for the deployment of new customer products;
- Testing and production environments are separate;
- New software, systems and developments are tested prior to release to the production environment.

H) Organisational Control.

- Sophos has a dedicated IT security team;
- The Risk and Compliance team manage internal risk reporting and controls, which include reporting on key risks to management;
- An incident response process identifies and remedies risks and vulnerabilities on a timely basis;
- Each new employee undertakes data protection and IT security training;
- The IT Security department conducts quarterly security awareness campaigns.

SOPHOS
Cybersecurity made simple.

Exhibit 3
Hosted Products

- Sophos Central
- Central Device Encryption
- Central Endpoint Protection
- Central Endpoint Intercept X
- Central Endpoint Intercept X Advanced
- Central Mobile Advanced
- Central Mobile Standard
- Central Phish Threat
- Central Intercept X Advanced for Server
- Central Server Protection
- Central Mobile Security
- Central Web Gateway Advanced
- Central Web Gateway Standard
- Central Email Standard
- Central Email Advanced
- Central Wireless Standard
- Any other Sophos product that is administered and operated via Sophos Central