Appropriate Filtering for Education settings

June 2021

Filtering Provider Checklist Reponses

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place*" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system*" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Sophos
Address	Abingdon Science Park, The Pentagon, Abingdon, OX14 3YP
Contact details	Nick.murphy@sophos.com
Filtering System	Sophos XGS Firewall
Date of assessment	25/11/2021

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Yes, Sophos is a member of the Internet Watch Foundation and routinely works with the IWF and other agencies in helping to identify the methods used by child abusers to share content, reporting the discovery of child abuse images online.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Yes, Sophos actively implements the IWF CAIC list.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, Sophos actively integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Sophos provides an "Intolerance and Hate" category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. Sophos recommends blocking this category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Sophos provides "Controlled Substances", "Marijuana" and "Legal Highs" categories that enable blocking of sites providing information about or promoting the use, trade or manufacture of drugs. Sophos recommends blocking these three categories.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Sophos provides an "Intolerance and Hate" category to enable blocking of sites that promotes terrorism and terrorist ideologies, violence or intolerance. Sophos recommends blocking this category.
Malware / Hacking	promotes the compromising of systems including anonymous		Sophos provides "Anonymizers", "Hacking, Phishing and Fraud",

	browsing and other filter bypass tools as well as sites hosting malicious content		"Spam URLs" and "Spyware and Malware" categories. Sophos recommends blocking these categories. In addition, all unencrypted content is scanned for malware. A cloud-delivered sandbox analyses any downloaded active content and blocks malware.
Pornography	displays sexual acts or explicit images		Sophos provides "Sexually Explicit", "Nudity" and "Extreme" categories. Sophos recommends blocking these categories. Also, Sophos provides "Safe-Search" enforcement on the major search engines. The option is also available to add a "Creative Commons" license that only shows images published under Creative Commons licensing laws. To date, using this method has not resulted in any pornographic images being forwarded to Sophos for reclassification.
Piracy and copyright theft	includes illegal provision of copyrighted material		Sophos provides "Peer to peer and torrents" and "intellectual piracy" categories. Sophos recommends blocking these categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Sophos provides the "Pro-suicide and self-harm" category. Sophos recommends blocking this category.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Sophos provides "Extreme" and "Criminal Activity" categories. Sophos recommends blocking these categories to block sites displaying or promoting the use of physical force intended to hurt or kill.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Sophos currently provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx. Sophos Labs enables us to dynamically update our web categories by providing a URL categorisation services that integrate Sophos URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database. Sophos classifies sites at the IP level, domain, sub-domain and path URL data is constantly reviewed and unclassified websites are classified on an hourly basis.

This is provided as a cloud delivered service to the Sophos appliance so they are always up-to-date with the latest classifications.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained .

Sophos XGS retain reports on box for up to a year. This is potentially impacted by disk space which is checked during the scoping phase with Sophos engineers. As the disk reaches its maximum capacity it will delete the eldest records. Therefore if the box has additional work to do that wasn't covered in the scoping its possible that the retention phase is reduced. It is possible to choose to use Central Reporting which would give 30 days of reporting with an XGS Xstream license, with increased licensing blocks available for purchase to meet a schools retention needs.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Sophos category database protects more than 400,000 organizations in more than 150 countries. The huge amount of data helps Sophos to fine tune our web filtering policies based on the typical activities of users in different settings. Sophos also provides tools that enable customers to create custom categories that over-ride current URL database classifications and end-users to request page reclassification, by the system administrator, directly from the block page. Education establishments can therefore tweak their web filtering policies to make sure they are enabling their staff and students to be the best and brightest they can be. Safe in the knowledge that they are also helping keep their users safe online.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Sophos can apply policy rules based on group information. If the school includes objects related to age then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the "Sex Education" category. Sophos also logs all user group activity separately for reporting. Reports can be generated for a specific event in a specific user group. All alerts can be sent using syslog into a Security Incident and Event Management system (SIEM).
• Circumvention – the extent and ability to identify and manage technologies and techniques used to		Sophos provides the "Anonymizers' category in our web filter. Sophos recommends blocking this category .

circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		Whilst we also provide a 'block filter avoidance app' application rule. Both policies would block users from being able to circumvent their filtering
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		The administration of the Sophos appliance is done by the school IT team (or partner if this is out-sourced). There is complete flexibility in the policy model to create policies that can block categories, file types, URLs, IPs and much more. Policies can be created easily and intuitively using a very user-friendly interface.
• Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter		The Sophos XG includes a content scanning feature, whereby URLs and web pages are dynamically analysed for specific keywords or phrases. Customers can upload multiple keyword lists to support different languages and provide better granularity. Any pages matching words or phrases contained within the keyword lists can be blocked and/or logged. In addition Administrators/Safeguarding officers can review the blocked keywords using the onboard log viewer and determine the context.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Sophos provides the rationale behind its web classification so that accurate choices can be made by IT administrators. This information can be found here: https://community.sophos.com/kb/enus/123333
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Sophos provides a management console that enables you to manage multiple sites in one console. Central policy can be configured and pushed out to your different sites. Whilst reporting and alerting can all be managed centrally.
• Identification - the filtering system should have the ability to identify users		Sophos can identify users transparently via Single-Sign on or through integration with directory server login processes. It can also provide non-transparent authentication where a user is required to login before browsing.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from		Sophos is able to filter all http and https connections. This is not limited to browser traffic and includes mobile

that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		and app connections. Sophos also provides policy-driven application control that can also identify and manage traffic that uses other protocols.
● Multiple language support – the ability for the system to manage relevant languages		Sophos supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		Sophos can be deployed as a standalone web proxy or in transparent bridge or gateway mode.
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school		For Windows and Mac devices that are not on the school network, web filtering can be enforced using our Sophos Central Endpoint protection client. This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (our Cloud management platform) and any violations can be reported on. There are over 48 categories that can be configured, as well as file type blocking. This includes sites that are on the IWF and Counter Terrorism Referral Unit block lists.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Sophos provides a number of built-in reports that can be used to see this information. These reports are fully customisable and can be emailed to admins/teachers/safeguarding officers. In addition the log files can be exported using syslog to third party tools.
● Reports – the system offers clear historical information on the websites visited by your users		Sophos provides a number of built-in reports that can be used to see this information. In addition the log files can be exported using syslog to third party tools.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Sophos has introduced Sophos Home (https://home.sophos.com). This provides home users free enterprise-grade security software to block malware and enforce parental category controls for web traffic. In terms of education, Sophos in partnership with SWGFL has produced thousands of educational booklets that redistributed to schools nationwide to advise on online safety. Sophos organises student days where we invite students into our headquarters in Abingdon to learn how Sophos deals with the latest online threats and what students can do to protect themselves more effectively. Many universities use Sophos products as part of their curriculum to learn about filtering and antimalware technologies.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Nick Murphy
Position	Education Account Executive
Date	25/11/2021
Signature	N. Murphy