

Appropriate Monitoring for Schools

June 2017



Provider Checklist Responses

Schools (and registered childcare providers) 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, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.



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. Children should not be able to access harmful or inappropriate material from the school or colleges 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.”

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

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is ‘appropriate’ for them.

Company / Organisation	Sophos PLC
Address	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP
Contact details	Oliver.Wells@Sophos.com
Filtering System	Sophos XG Firewall
Date of assessment	01 August 2017

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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		Yes, Sophos works with CTIRU and incorporates this list into the URL database.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		Sophos provides a "Criminal Activity" category that filters and reports on web content that is illegal including child abuse images and unlawful terrorist content.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Sophos provides keyword analysis using custom dictionaries on social media messages and posts, web searches and webmail. It will detect and report on bullying keywords as defined by the system administrator.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Sophos provides keyword analysis using custom dictionaries on social media messages and posts, web searches and webmail. It will detect and report on child sexual exploitation keywords as defined by the system administrator.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Sophos provides an "Intolerance and Hate" category to enable blocking and reporting 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.
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.
Self Harm	promotes or displays deliberate self harm		Sophos provides the "Pro-suicide and self-harm" category. Sophos recommends blocking this category.
Suicide	Suggest the user is considering suicide		Sophos provides the "Pro-suicide and self-harm" and "Criminal Activity" categories to monitor and report on users considering suicide. Sophos recommends blocking these categories.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Sophos provides "Extreme" and "Criminal Activity" categories to monitor and report on users considering violence. 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 88 different URL categories. For the full list see: <https://www.sophos.com/threat-center/reassessment-request/utm.aspx>. Sophos Labs provides 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 and 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.

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

The Sophos category database is in use on over 300 million devices worldwide. This provides a uniquely large user community that reports category misclassification requests directly to Sophos. Currently, fewer than 50 of these requests are made per day. This lack of customer complaint demonstrates clearly that the Sophos category database is of the highest standard. Furthermore, the majority of the reported URLs are not reclassified as Sophos ordinarily determines the original classification is correct.

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.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none">Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to		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. Additionally, all alerts can be sent using syslog into a Security Incident and Event Management system (SIEM).

<ul style="list-style-type: none"> • BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location 		<p>Sophos can be deployed in transparent mode to monitor school guest wi-fi. Administrators can choose to use a captive portal service where the user must login to gain web access. Monitoring does not extend outside the school wi-fi with this Sophos solution but this can be achieved by integrating with other Sophos products if required.</p>
<ul style="list-style-type: none"> • Data retention –what data is stored, where and for how long 		<p>Sophos keeps reporting data for 3 years and logs for 48 hours. Options to store all data permanently are also available.</p>
<ul style="list-style-type: none"> • Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers 		<p>No software is required on devices. If monitoring is required outside the school, a low impact software agent is installed on each device.</p>
<ul style="list-style-type: none"> • Flexibility – schools ability to amend (add or remove) keywords easily 		<p>Key words can be added and removed from custom lists easily.</p>
<ul style="list-style-type: none"> • Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools? 		<p>Users can be shown an initial custom web page stating the school monitoring policy. Sophos provides many guidance and advice documents to support schools.</p>
<ul style="list-style-type: none"> • Multiple language support – the ability for the system to manage relevant languages? 		<p>Sophos supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.</p>
<ul style="list-style-type: none"> • Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process? 		<p>Sophos provides a customisable dashboard where administrators can view and then respond to immediate issues. Additionally, reports can be scheduled frequently throughout the school day to provide a near real-time view and enable a rapid response.</p>

- Reporting – how alerts are recorded within the system?

Sophos records all web traffic logs for 48 hours then aggregates this data and stores it for three years.

Please note below opportunities to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

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 anti-malware technologies.

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	ALI KENNEDY
Position	DIRECTOR
Date	23/8/17
Signature	