UK Safer Internet Centre
www.saferinternet.org.uk

Appropriate Filtering for Education settings

June 2016

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"*[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated 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 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	The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP
Contact details	Spencer Parker, Product Line Manager, Web (spencer.parker@sophos.com 07929 055430)
Filtering System	Sophos XG UTM Appliance V16.0
Date of assessment	5th October 2016

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	🟨

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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

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
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)	🟩	Yes
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Yes

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 has an "Intolerance and Hate" category where we categorize websites which fall into these categories and we would recommend the blocking of this category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Sophos includes a controlled substances category in its URL data. We also have additional categories for "legal highs" and "Marijuana" and we would recommend the blocking of all three of these categories for schools.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Sophos includes these in our "Intolerance and Hate" category.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	Sophos provides a number of categories to cover this. These are Anonymizers, Hacking, Phishing and Fraud, Spam URLs, and Spyware & Malware. In addition Sophos utilizes it anti-malware engines on all unencrypted content to detect malicious content. As an option, Sophos also offers a cloud-sandboxing solution called Sophos Sandstorm which takes any downloaded active content (e.g. executables or files with active content such as PDF or

		🟩	office documents with macros) which is not convicted straight away by the anti-malware engines and sends it to a cloud sandboxing solution which runs the content in a safe remote environment to check for any malicious intent.
Pornography	displays sexual acts or explicit images	🟩	Sophos includes these in our "Sexually Explicit", "Nudity" and "Extreme" categories. In addition Sophos provides Safe-search enforcement on the major search engines, and has a two level safe search on Images where we can optionally add in a "creative commons" license which would only show images published under creative commons licensing laws. To date this level has not returned any pornographic images that have been forwarded to Sophos for reclassification.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Sophos provides a number of categories which we would recommend you block to achieve this on the Sophos XG UTM. Sites which list pirated content for sharing by peer to peer or by file locker solutions can be found in the "peer to peer & torrents" or "intellectual piracy" categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Sophos currently includes self harm sites in our "Pro-suicide and self-harm" category.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Sophos provides both an "Extreme" category, and a "Criminal Activity" pair of categories and recommends blocking these.

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

Sophos Labs provides URL categorization services which integrates Sophos' own URL data with that of many third party suppliers (e.g. IWF, CTIRU) to provide a class-leading URL database. Currently Sophos XG UTM appliance provides 88 different categories (for the list see https://csc.cyberoam.com/cyberoamsupport/webpages/webcat/viewallcategorydescription.jsp) to choose from and we classify sites at the IP level, domain, sub-domain and path so we get the correct classifications for the pages you are visiting. We are constantly reviewing our URL data and the top unclassified websites are classified on an hourly basis. Sophos then provides this as a cloud service to our appliances so they always received the latest classifications for the URLs visited.

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

Sophos' category database is in use on over 300M devices worldwide which provides us a very large user community that report to us any misclassifications in our database. As we receive less than 50 of these requests per day (and most of which we do not reclassify as we believe them to be correct) we know the quality of our database is of the highest standard. We also provide a number of tools in the solution which help our customers. These include internal reclassification requests directly from the block page itself that go to the administrator of the solution to check if required and also the ability to create your own custom categories which override the current classifications from the URL database.

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 XG UTM has the ability to generate policy rules based on group information. If the school includes objects in their directory that relate to age, then policies can be created that open up certain categories of websites once a certain year has been reached (e.g. sex education category). We also log all the groups of a user for reporting and these groups can be used to create reports for certain types of event. All alerts can also be sent out of the appliance via Syslog into almost any other alert monitoring system.
● 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 filtering solution is done by the school IT team (or one of their partners if this is out-sourced) and they have complete flexibility in the policy model to create a policy that can block categories, file types, URLs, IPs, and much more in an extremely user-friendly UI.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Sophos does not supply a recommended filtering policy for schools as it believes the school itself should create this. What we

	🟩	do provide is a rationale behind our web classification so accurate choices can be made by the IT admins around this. This information can be found at https://csc.cyberoam.com/cyberoamsupport/webpages/webcat/viewallcategorydescription.jsp
- Identification - the filtering system should have the ability to identify users	🟩	The Sophos XG UTM has a multitude of different ways of identifying users, both transparent (e.g. NTLM or SAML) and non-transparent (e.g. Captive portal)
- Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies	🟩	As the Sophos XG UTM can be deployed in a transparent mode, adding this to the guest Wi-Fi provided by schools is easy. Identifying the users is not so easy though, so you can choose to use a captive portal where the user would have to login first to be able to surf the web. If HTTPS decryption is deployed, the block page can show the certificate that needs to be added to the mobile device and instructions given on how to add this to the mobile device so the alerts are no longer seen. However, attempting to do HTTPS decryption on many mobile apps actually breaks them as they employ certificate pinning and you cannot decrypt their traffic. These would have to be manually added to the HTTPS decryption exceptions if the school wanted to allow the use of this app. Also this would not cover the device if it were using cellular (e.g 3G) data services, or if it leaves the school and uses another network (e.g. home broadband) for use.
- Multiple language support – the ability for the system to manage relevant languages	🟩	Yes, we support multiple block pages if we detect the language of the browser and custom block pages where you want to include multiple languages on the same page.
- Network level - filtering should be applied at 'network level' ie, not reliant on any	🟩	Sophos XG UTM can be deployed as a standalone web proxy or in

software on user devices	🟩	transparent bridge mode.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Sophos XG UTM contains a number of inbuilt reports which can be used to see this information. In addition, the raw log files can be exported via Syslog to third party tools.
● Reports – the system offers clear historical information on the websites visited by your users	🟩	Sophos XG UTM contains a number of inbuilt reports which can be used to see this information. In addition, the raw log files can be exported via 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".*[3]

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

Sophos has introduced Sophos Home (https://home.sophos.com) which provides home users free endpoint security software to block malware and enforce parental category controls for web traffic. This provides Enterprise-grade security free for home users that outperforms all other free anti-malware solutions and almost all paid-for solutions too.

In terms of education, Sophos in partnership with SWGFL have produced thousands of online educational booklets that are given to thousands of schools across the country to advise on online safety.

We also have student days at Sophos where we invite students into our head office in Abingdon to learn how Sophos deals with the latest online threats, and what students can do to better protect themselves.

It is also worth noting that many universities use Sophos products as part of their studies to learn about filtering and AV technologies

[3] 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	STUART HILLINGHAM
Position	DIRECTOR
Date	14/10/16
Signature	