Appropriate Filtering for Education settings

May 2023

Filtering Provider Checklist Reponses

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 and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] 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*."

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	Wave 9 Managed Services Limited
Address	1 Hargreaves Court, Staffordshire Technology Park, Stafford ST18 0WN
Contact details	Andy McFarlane (Director) andy.mcfarlane@wave9.co.uk
Filtering System	WaveConnect Education Broadband – Sophos XGS
Date of assessment	8.1.24

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		Wave 9 and Sophos are Members of the Internet Watch Foundation
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Yes, WaveConnect actively implements the IWF URL list
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, WaveConnect actively integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
• Confirm that filters for illegal content cannot be disabled by the school		Wave 9's standard service offer is a fully managed service, and therefore filters for illegal content cannot be disabled by the school. However, Individual schools/trusts may request that appropriately skilled technical staff, as part of their local service provision and operating model, have management access to the filter for day-to-day policy administration based on an assessment of risk. We do not deny management access if requested, so in this scenario, filtering policies may be changed locally. It is important to note, non-authorised staff or students do not have the ability to disable any feature on the firewall or web filter.

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		Our standard deployment for Education would block the

	grounds of race, religion, age, or sex.		category “Intolerance and Hate” which would cover content that promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex. This category is included in our default Safeguarding list.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Our standard deployment for Education would block the category “Controlled substances category” along with “Legal highs” and “Marijuana” which cover content that displays or promotes the illegal manufacture, trade or use of drugs or substances. This category is included in our default Safeguarding list.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Our standard deployment for Education would block the category “Intolerance and Hate” It would also block the category “Criminal Activities” which would include the “Counter Terrorism Internet Referral Unit” list. This would cover sites that promote terrorism and terrorist ideologies, violence, or intolerance. This category is included in our default Safeguarding list.
Gambling	Enables gambling		Wave 9 standard deployments would block any website which falls under the Gambling category, for all user-types, be they staff or student. If no user-based-filtering is performed or possible, the Gambling category is blocked by the unauthenticated web policy.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Wave 9 provides an “Anonymizers”, “Hacking, Phishing and Fraud”, “Spam URLs” and “Spyware and Malware” categories. Wave 9 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. This category is included in our default Safeguarding list.
Pornography	displays sexual acts or explicit images		Wave 9 provides "Sexually Explicit", "Nudity" and "Extreme" categories. Wave 9 recommends blocking these categories. Also, Wave 9 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. These categories are included in our default Safeguarding list.
Piracy and copyright theft	includes illegal provision of copyrighted material		Wave 9 standard deployments would block sites supporting, enabling, or engaging in sharing of content that is protected intellectual property and websites that provide, distribute or sell school essays, projects, or diplomas
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Wave 9 standard deployments would block Sites promoting suicide and self-harm. These categories are included in our default Safeguarding list.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Wave 9 provides "Extreme" and "Criminal Activity" categories. Wave 9 recommends blocking these categories to block sites displaying or promoting the use of physical force intended to hurt or kill. These categories are included in our default Safeguarding list.

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

The system 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.

We classify sites at the IP, domain, sub-domain level 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-todate 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.

Data retention is at the discretion of the customer and beyond any policy requirements (E.g. the GDPR) policy is only limited by the storage capacity of the schools filtering appliance and any archive logs they may choose to keep. The school is the data controller and so should determine their data retention requirements in line with their policy.

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

Our database is in use on over 300 million devices worldwide. This provides a uniquely large user community that reports category misclassification requests directly to the service.

Currently, fewer than 50 of these requests are made per day. This lack of customer complaint demonstrates clearly that the category database is of the highest standard. Furthermore, most of the reported URLs are not reclassified as review ordinarily determines the original classification is correct.

We also provide 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 or via the Wave 9 Helpdesk.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff		Wave 9 can apply policy rules based on group information, usually the schools Active Directory. If the school includes objects related to age, year group, role then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the “Sex Education” category). Wave 9 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 a syslog into a security incident and event management system (SIEM).
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		Wave 9 provides the "Anonymizers' category in our web filter. Wave 9 recommends blocking this category . 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. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		Our service is coadministered with the establishment allowing nominated members of staff control of the filter policies or assistance from our qualified helpdesk staff. Temporary "unblocking" can be achieved "ad-hoc" at the discretion of the school by an authorised member of staff.
● 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, this would include AI generated content. 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		Our Service Level Agreement (SLA) outlines the default polices applied with our service. Any changes to these are agreed

		with the establishment dependent on school context and assessment of risk. Our rational is published in our "Security, Safeguarding and Prevent" documentation for WaveConnect Education service.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Wave 9 can provide a management console that enables the customer to manage multiple sites in one console. Central policy can be configured and pushed out to multiple sites. Whilst reporting and alerting can all be managed centrally.
● Identification - the filtering system should have the ability to identify users		Our services as a multitude of different ways of identifying users, both transparent (e.g. NTLM or SAML) and non-transparent (e.g. Captive Portal). Typically, we use "Active Directory" single sign-on to identify users
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from 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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps		Our service can be deployed in transparent mode, adding this to the "Guest" Wi-Fi provided by the establishment can be easily achieved. Users need to be identified by the use of the "Captive Portal", users must authenticate first. If HTTPS decryption is deployed, the block page can display the security certificate that needs to be deployed to the mobile device(s) and instructions on how to install the security certificate on the mobile device so alerts are no longer seen. However, deploying HTTPS to many APPS may have an adverse effect as they employ "certificate pinning" and may not allow decryption. In

		this case, an HTTPS decryption exception will need to be added manually with the support of our Helpdesk staff, which is included within the WaveConnect Education support SLA. Please note that this does not cover 3G/4G cellular data services or devices not connected to the establishment's internal network (e.g. home broadband)
● Multiple language support – the ability for the system to manage relevant languages		Wave 9 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)		Our service does not require any client based software.
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		We have three options addressing remote working that schools can opt for depending on the extent to which this applies to a particular establishment. At a based level all our services include remote access VPN as standard and when enforced by device management all traffic is router via the school based web filter. A second option is to enforce a filtering policy using the Sophos Central Endpoint protection client. This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (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. For schools where there are large numbers of student devices being used at home and in school, we can deliver the option of filtering and monitoring using an agent based solution based on Lightspeed.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		There is the ability to report inappropriate content via a web portal or by request to our help desk.
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		A range of standard and customisable reports can be viewed or automated by email that shows user activity.
• Safe Search – the ability to enforce 'safe search' when using search engines		SafeSearch is enforced by both the Authenticated and Unauthenticated web policies for the search engines google.com/uk, bing.com and yahoo.com/uk. All other search engines are blocked, thus providing only Safe Search entry points to those search engines where Safe Search enforcement is possible.

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

Wave 9 is 100% focussed on the provision of safe, secure Internet connectivity and infrastructure to Education. Our leadership team have been involved in the provision of internet and filtering services to education since the late 1990's.

Our services are designed and delivered in a way that ensures our school customers benefit from a service that exceeds the requirements set out in Annex C of KCSIE September 2021.

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

We recognise that over and above the deployment of appropriate technical infrastructure, online safety is about education and awareness.

We work with a number of partners, including Sophos, to actively signpost, distribute and promote online safety information and resources. We work with our school customers to help develop their knowledge, understanding and practice.

We have recently supported the Royal Air Force with their STEM bus project that includes topic such as online security.

We also actively promote the 360-degree safe programme and safer internet day.

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	Andy McFarlane
Position	Director
Date	8.1.24
Signature