Appropriate Filtering for Education settings

June 2020

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. 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."

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	Wave 9 Managed Services Limited
Address	1 Hargreaves Court, Staffordshire Technology Park, Stafford ST18 0WN
Contact details	Andy McFarlane (Operations Director) andy.mcfarlane@wave9.co.uk
Filtering System	WaveConnect Education Broadband – Sophos XG
Date of assessment	1.8.2020

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		Our filtering platform is provided by Sophos who are IWF members. Wave 9 is not currently a member.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Yes, Wave 9 actively implements the IWF CAIC list
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, Wave 9 actively integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

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.		Our standard deployment for Education would block the 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.
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.
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.

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.
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. To date, using this method has not resulted in any pornographic images being forwarded to Wave 9 for reclassification.
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.
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.

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

Using the Sophos Platform Wave 9 provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx. Wave 9 provides URL categorisation services that integrate Wave 9 URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database. Wave 9 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 Wave 9 appliance so they're 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.

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

The Wave 9 database is in use on over 300 million devices worldwide. This provides a uniquely large user community that reports category misclassification requests directly to Wave 9. Currently, fewer than 50 of these requests are made per day. This lack of customer complaint demonstrates clearly that the Wave 9 category database is of the highest standard. Furthermore, the majority of the reported URLs are not classified as Wave 9 ordinarily determines the original classification is correct. Wave 9 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 or via the Wave 9 Helpdesk.

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		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		Our service is co-administered with the establishment allowing nominated members of staff control of the filter policies or assistance form our qualified helpdesk staff. Temporary "unblocking" can be achieved "ad-hoc" at the discretion of the school by an authorised member of staff. All changes are logged in the "Change Log" to ensure who and when changes where applied are recorded.
● 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)		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		Our service does not require any client based software.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Wave 9 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.
● Reports – the system offers clear historical information on the websites visited by your users		A range of standard and customisable reports can be viewed or automated by e-mail that shows user activity. A change log is also maintained that records and changes made to the system configuration.

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 2019.

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.

[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	Andy McFarlane
Position	Operations Director
Date	1.8.20
Signature