Appropriate Filtering for Education settings

June 2017

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
Contact details	Andy McFarlane (Operations Director) andy.mcfarlane@wave9.co.uk
Filtering System	WaveConnect Sophos UTM 9
Date of assessment	1.9.17

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		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 CAIC list)		Yes, our services actively implement the IWF CAIC List.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, Our service 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		Our service provides several categories to cover this. These are Anonymizers, Hacking, Phishing and Fraud, Spam URLs and Spyware and Malware. In addition the Sophos platform utilises Anti-Malware engines on all unencrypted content to detect malicious content.
Pornography	displays sexual acts or explicit images		Our service includes "Sexually Explicit", "Nudity" and Extreme" categories. In addition, Safe-Search is enforced on all major search engines. We offer a two-level safe search on images where we can optionally add in a "Creative Commons" license which would only display images published under creative commons licensing laws.
Piracy and copyright theft	includes the illegal provision of copyrighted material		Our service provides the ability to block sites which list "Pirated" content for sharing Peer to Peer or by file locker solutions that can be found in the "Peer to Peer and torrents" or "Intellectual Piracy" categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Our services provide the ability to block "Self-Harm" sites in our "Pro-Suicide and Self-Harm" categories.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Our service provides both an "Extreme" category, and a "Criminal Activity" category. We recommend blocking these.

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 our WaveConnect service provides 88 different URL Categories;

The full list can be found at http://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.

Customers have the option to tailor which categories are blocked for different user groups such as staff or students. This can be done locally or through the Wave 9 service desk where filtering changes are part of the WaveConnect service.

Our service classifies sites at the IP Level, domain, sub-domain and path. Data is constantly reviewed and updated on an hourly basis and applied to our customer's service.

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

The category database use in the WaveConnect service is in use on over 300 million devices worldwide. The provides a uniquely large user community that is able to report category misclassification requests directly, fewer than 50 requests are made per day. Our service desk reacts quickly to request to unblock sites within a service level agreement (if the school does not want to manage this locally) so that any disruption to teaching and learning is avoided. Customers have the option to tailor which categories are blocked for different user groups such as staff, students or key stages to ensure that the level of filtering is appropriate.

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		Age appropriate filtering can be achieved through integration with the establishments "Active Directory" structure. Age group specific filtering policies are applied, this can be based on role, key stage, class or individual users.
• 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.
• 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		Our service includes support for multiple block pages if we detect the language of the “Browser”. Custom block pages can be configured where multiple languages may be 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		Full reporting is provided on appropriate and inappropriate blocked or allowed content.
● 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 2016.

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	1.9.17
Signature