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	Cisco Meraki
Address	
Contact details	
Filtering System	Cisco Meraki Content Filtering – Data provided by Webroot
Date of assessment	November 10, 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 for that question is AMBER.	

[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

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		Both Webroot and Cisco are members of IWF. Also, Webroot is the endpoint security provider for the IWF.
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The CAIC list is added to Webroot's primary URL filtering database file daily, which is then distributed to filtering customers on a real-time basis. The URLs on this list are categorized as Adult and Pornography, in order to be blocked.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Webroot is currently working with the Counter Terrorism unit and Home Office on acquiring and integrating this list. This list will be integrated into Webroot's primary database file daily, which is then distributed to filtering customers.

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.		Through policy-based filtering, inappropriate online content can be blocked through the following category(ies): • **Hate and Racism** - Sites that contain content and language in support of hate crimes and racism.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		• **Abused Drugs** - Discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. Information on "legal highs": glue sniffing, misuse of prescription drugs, or abuse of other legal substances. • **Marijuana** - Marijuana use, cultivation, history, culture, and legal issues.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		• **Illegal** - Criminal activity, how not to get caught, copyright and intellectual property violations, etc. • **Hate and Racism** - Sites that contain content and language in support of hate crimes and racism. • **Weapons** - Sales, reviews, or descriptions of weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		• **Malware Sites** - Malicious content including executables, drive-by infection sites, malicious scripts, viruses, Trojans, and code. • **Phishing and Other Frauds** - Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. • **Proxy Avoidance and Anonymizers** - Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering. • **Spyware and Adware** - Spyware or Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization. Also, unsolicited advertising popups and programs that may be installed on a user's computer. • **Hacking** - Illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs that may allow compromise of networks and systems. Avoidance of licensing

			and fees for computer programs and other systems.
Pornography	displays sexual acts or explicit images		• **Adult and Pornography** - Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including newsgroups and forums, which are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art.
Piracy and copyright theft	includes illegal provision of copyrighted material		• **Shareware and Freeware** - Software, screensavers, icons, wallpapers, utilities, ringtones. Includes downloads that request a donation, and open source projects. • **Peer to Peer** - Peer to peer clients and access. Includes torrents, music download programs. • **Illegal** - Criminal activity, how not to get caught, copyright and intellectual property violations, etc.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		• **Violence** - Sites that advocate violence, depictions, and methods, including game/ comic violence and suicide. • **Gross** - Vomit and other bodily functions, bloody clothing, etc.
Violence	Displays or promotes the use of physical force intended to hurt or kill		• **Violence** - Sites that advocate violence, depictions, and methods, including game/ comic violence and suicide.

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

A complete list of Webroot URL categories, including descriptions and sample URLs for each category is available at http://brightcloud.com/tools/change-request-url-categorization.php for review. To date, the Webroot BrightCloud Web Classification service has categorized over 27 billion URLs (over 95% of the known Internet) across 83 categories, allowing administrators to finely tune security and policy settings to keep children away from unwanted content. Through

real-time updates and cloud calls, Webroot provides updated classification data to ensure that classification information is accurate and up-to-date.

Because the list of potentially inappropriate content above is not exhaustive, administrators can configure and tune their individual devices to provide the appropriate level of access based on their organization's internal policies. Also, integration with Google, Yahoo, and Bing SafeSearch further enables a safe and secure internet environment. YouTube for Schools and YouTube EDU integration also provides an additional layer of security.

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

When filtering, granularity is always an important consideration. Because there are 83 categories to choose from, along with other configuration options, such as blacklisting and whitelisting, unreasonable restrictions on content can be avoided, ensuring that students have access to online learning resources and materials. Further, when a device attempts to access a web page, the address is checked against a database of URIs. Addresses are passed through a series of pattern matching steps so that, for example, access to a specific URL on a website may be allowed, with others excluded. Specific URL addresses can be added to a whitelist to take precedence over the filter.

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		Different filtering policies can be applied to clients by VLAN, Active Directory group, manually, or via endpoint management software integration.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Intuitive GUI-based configuration allows for point and click filtering setup of over 80 categories as well as blocking or whitelisting of specific sites or URI patterns.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		As filtering approaches need to be flexible enough to address a variety of use cases and educational environments, we do not provide a recommended filtering approach but rather allow educational institutions to tailor their filtering policies to their needs. Customizable filtering policy application by device, user, or group allows

		administrators to minimize the risk of over-blocking.
• Identification - the filtering system should have the ability to identify users		Native Active Directory integration allows for identification, policy application, and reporting based on user.
• Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		Layer 7 firewalling allows for blocking of applications, application categories and URLs by non-HTTP/HTTPS requestors such as apps.
• Multiple language support – the ability for the system to manage relevant languages		The system supports blocking in multiple languages. Multi-language management is currently in the development roadmap.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		Filtering is applied as network traffic passes through the security appliance at the perimeter of the network, with no endpoint software required.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Native splash page support allows administrators to configure a splash page that informs users of who to contact to report inappropriate content or access.
• Reports – the system offers clear historical information on the websites visited by your users		All block events are reported natively in the web management console, and can also be exported via Syslog. URL and application logging are also available for non-blocked traffic.

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

Cisco works extensively with schools and organizations to provide solutions and teach children about how to be safe online. We also produce and distribute solution documents, such as the following: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/screen.pdf

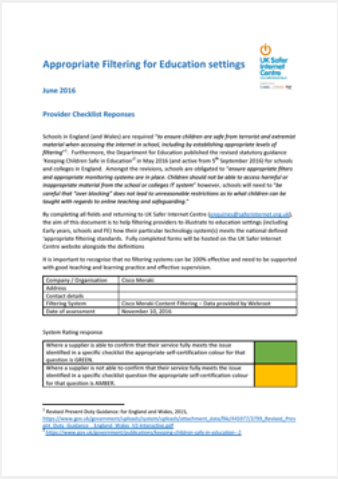
[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

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	Todd Nightingale
Position	SVP, GM
Date	Dec 22, 2016
Signature	Todd Nightingale (Dec 22, 2016)


Appropriate Filtering for Education settings

June 2016

Provider Checklist Reponses

UK Content Filtering Certification

Adobe Sign Document History 12/22/2016

Created:	12/09/2016
By:	Sean Butler (sean.butler@meraki.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAANryYAvZ1bMXH1wAi9j4kwSQZfzAF_Pkk

"UK Content Filtering Certification" History

Document created by Sean Butler (sean.butler@meraki.com)
12/09/2016 - 4:03:01 PM PST- IP address: 192.195.83.200

Document emailed to Todd Nightingale (tnight@cisco.com) for signature
12/09/2016 - 4:03:55 PM PST

Document e-signed by Todd Nightingale (tnight@cisco.com)
Signature Date: 12/22/2016 - 1:29:35 PM PST - Time Source: server- IP address: 192.195.83.200

Signed document emailed to raviv.levi@meraki.net, Todd Nightingale (tnight@cisco.com) and Sean Butler (sean.butler@meraki.com)
12/22/2016 - 1:29:35 PM PST