Appropriate Filtering for Education settings

June 2021

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*" and they "should be doing all that they reasonably can to limit children's exposure to the above 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."

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	Webroot
Address	385 Interlocken Crescent, Suite 800, Broomfield, CO 80021, USA
Contact details	(800) 772-9383 – jonathanb@opentext.com
Filtering System	Webroot DNS Protection, DNS Filtering
Date of assessment	10/11

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		Webroot has been a member of the IWF since 2011
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Webroot DNS Protection blocks domains contained in the IWF URL list under the categories of "Illegal" and **"Adult and Pornography"** which include Child Abuse images.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Domains in the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' (CTIRU list) are classified as **"Illegal"** and blocked by default.

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.		DNS Protection Policies include a **"Hate and Racism"** Domain Category which includes domains that contain content and language in support in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		DNS Protection Policies include an **"Abused Drugs"** Domain Category which includes 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.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		DNS Protection Policies can include domains that contain this type of content when the following categories are selected: • **"Illegal"** (Criminal activity, how not to get caught, copyright and

			intellectual property violations, etc.). • **"Violence"** (Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.) • **"Hate and Racism"** (content and language in support of hate crimes and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.). • **"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		DNS Protection Policies can include domains that contain this type of content when the following categories are selected: • **"Proxy Avoidance and Anonymizer**" (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.) • **"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.) • **"Malware"** (Malicious content including executables, drive-by infection sites, malicious

			scripts, viruses, trojans, and code.) • **"SPAM URLs"** (URLs contained in SPAM) • **"Phishing and Other Frauds"** (Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. • **"Bot Nets"** (These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts) • **"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.)
Pornography	displays sexual acts or explicit images		DNS Protection Policies include a **"Adult and Pornography"** domain category which includes content which contains 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, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, strip clubs, and sexually explicit art.

Piracy and copyright theft	includes illegal provision of copyrighted material		DNS Protection Policies include an **"Illegal"** domain category which includes content which contains 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)		DNS Protection Policies include a **"Violence"** domain category which includes domains that advocate violence, depictions, and methods, including game/comic violence and suicide.
Violence	Displays or promotes the use of physical force intended to hurt or kill		DNS Protection Policies include a **"Violence"** domain category which includes domains 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

Webroot DNS Protection provides administrators the ability to assign filtering policies to networks or individual devices. Each policy has 80 available categories that can either be allowed or blocked based on the filtering requirements. When a domain is requested that is selected to be filtered (blocked), instead of returning the requested IP address, the IP address of a block page is returned, thereby protecting the user and device from possibly harmful content.

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.

Each DNS request is logged and can optionally include the requesting username, device, domain, and requesting IP address. These logs are available for reporting for up to 3 months with a maximum retention period of 1 year, after which the data is then deleted / purged.

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

Webroot DNS Protection policies can be fully customized by selecting from 80 different categories. Additionally, exceptions, both allow and block, can be applied to finetune policies based on need. Policies can be applied to individual systems, groups of systems and networks.

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		Webroot DNS Protection policies can be fully customized by selecting from 80 different categories for different age groups. Policies also include the ability to apply SafeSearch functionality for Search Engines to remove explicit content. Policies can be applied to individual systems, groups of systems and networks.
● 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.		DNS Protection Policies include a **"Proxy and Avoidance"** Domain Category which includes Proxy servers and other methods to gain access to domains in any way that bypasses domain filtering or monitoring including web-based translation sites that circumvent filtering. **DoH Providers** are classified as "Proxy and Avoidance" and DNS Protection takes additional steps to make sure DoH providers are correctly identified and blocked. VPNs can be individually blocked by domain.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Filters are fully customizable depending on need.
● 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. For example, being able to contextually analyse text on a page and dynamically filter		Webroot DNS Protection filters domains based on the assigned category.
● Filtering Policy – the filtering provider publishes a rationale that details their		Webroot DNS Protection leverages BrightCloud

approach to filtering with classification and categorisation as well as over blocking		Web Classification. All categories are published including descriptions and examples.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Webroot DNS Protection is designed to protect individual systems, groups of systems and entire networks. Central policies can be configured and applied across multiple sites or down to individual systems through the Webroot Management Console which provides dashboards and assist with oversight.
• Identification - the filtering system should have the ability to identify users		When running the Webroot DNS Protection Agent, the username associated with each DNS request as well as the domain requested is logged. Comprehensive reporting is then available through the Webroot Management console. All data is also exposed through the rest-based Webroot Unity API in order to integrate into any desired reporting platform.
• 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)		Webroot DNS Protection can apply filtering to entire networks and hotspots, providing filtering for mobile devices when connected to a protected hotspot. As filtering occurs at the DNS layer, mobile applications can be controlled based on request category.
• Multiple language support – the ability for the system to manage relevant languages		Webroot DNS Protection filters based on domain category regardless of language.

● 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)		DNS filtering can be configured at the 'Network Level'. When DNS requests are sent to the Webroot DNS resolvers, the requests are filters based on the policy associates with the requesting WAN IP address. In this way, all devices on the network or Wi-Fi hotspot can be protected through DNS Protection.
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school		In order to extend protection beyond the Network Level, Webroot DNS Protection provides an intelligent agent that will filter DNS requests on every network through which the device is connected. The agent provides remote protection as well as logging for all DNS requests made.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Access to reporting is available through the Webroot Management Console as well as through the rest-based Unity API, providing visibility to any inappropriate content that may have been accessed, as well as historical data as to what DNS requests were made.
● Reports – the system offers clear historical information on the websites visited by your users		Comprehensive reporting is available through the Webroot Management console. All data is also exposed through the rest-based Webroot Unity API in order to integrate into any desired reporting platform.

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

Webroot works closely with education institutions and the MSPs that support them. Based on this, the DNS Protection solution has expanded to help schools easily implement and manage SafeSearch functionality. Webroot is also a longstanding member of the IWF and is the trusted Endpoint security provider for the IWF.

[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
- 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	Jonathan Barnett
Position	Product Manager – Webroot DNS Protection
Date	October 11, 2021
Signature