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	Barracuda Networks, Inc.
Address	3175 Winchester Blvd, Campell, California 95008, USA
Contact details	+44 118 338 4600
Filtering System	Barracuda Web Security Gateway Barracuda SecureEdge Barracuda CloudGen Firewall
Date of assessment	March 2024

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		Active Member
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Part of the Barracuda Web Categorization Service
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Part of the Barracuda Web Categorization Service
• Confirm that filters for illegal content cannot be disabled by the school		Filtering and monitoring of illegal content can only be disabled with local admin rights.

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.		**Webfilter Category "Hate or Slander".** Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		**Webfilter Category "Illegal Drugs".** Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		**Webfilter Categories "Terrorism or Extremists".** Any site that promotes, instructs, or advocates terrorism or extremism.

			Webfilter Categories "Hate or Slander". Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice.
Gambling	Enables gambling		**Webfilter Categories "Gambling in Gerneral".** All online and offline gambling, and sites that promote gambling skills and practice.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		**Webfilter Categories "Malware"** and "Hacking or Cracking". Resources for the illegal or questionable use of computer hardware or software are included here. Sites that describe how to gain unauthorized access to systems and that distribute copyrighted material that has been cracked to bypass licensing.
			Webfilter Categories "Hacking or Cracking". Resources for the illegal or questionable use of computer hardware or software are included here. Sites that describe how to gain unauthorized access to systems and that distribute copyrighted material that has been cracked to bypass licensing.
Pornography	displays sexual acts or explicit images		**Webfilter Category "Adult Porn".** Sites containing sexually explicit content in an image-based or textual form. Any other form of adult/sexually-oriented material is also listed here.

			Additional Subcategories in "Adult Material" are: - **Adult Magazines or News** - **Adult Search or Links** - **Fetish** - **Nudity** - **Sexual Expression** - **Sexual Services** The educational **Webfilter Category "Sex Education"** which are sites that discuss sex and sexuality in an informative and non-voyeuristic way can be allowed, blocked, reported or monitored.
Piracy and copyright theft	includes illegal provision of copyrighted material		**Webfilter Category "Piracy & Copyright Theft".** Sites that are clearly distributing copyrighted material in violation of the copyrights.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		**Webfilter Categories "Self-Harm" and "Violence or Suicide".** Sites that contain examples or promotion of self-harm. This includes suicide, N/A cutting, and advocacy of eating disorders or euthanasia.
Violence	Displays or promotes the use of physical force intended to hurt or kill		**Webfilter Category "Violence or Suicide".** Any site that displays or promotes content related to violence against humans or animals is placed in this category, as are sites that advocate any means of harming oneself such as self-mutilation or euthanasia.

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

The Barracuda Web Categorization is a Barracuda Networks website categorization service that organizes domains into content categories (subcategories) which are grouped below by

supercategories. When you create rules that block categories of websites, you can choose a supercategory to block, or you can drill down and block websites at the subcategory level. WCS provides very granular categorization so that you can create fine-grained browsing policies for content, and create granular reports on user browsing activity. In the event that a specific URL is currently not present in the cloud-based database, the service initiates a connection to the destination website and attempts to categorize it based on the observed content. Content such as text, meta-data, links and pages following those links help us to categorize a URL/IP automatically. Once categorized, it is put provisionally into the database and will be reviewed by our categorization team in due course.

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.

In general we support a data retention time of at least 3 months. For longer data retention we recommend the usage of external syslog collectors.

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

Our web-categorisation service allows for fine grained acceptable browsing policies. In addition, some users can be deterred from browsing to content deemed inappropriate by simply providing a “Warn” splash screen, reminding users that their browsing is tracked and logged but not blocked.

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		Users can be grouped in any specifically required way and used in the web filter policies.
• 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.		The webfilter categories “Remote Proxies”, “DoH & DoT” and “VPN” provide the possibility to block web-based policy circumvention attempts. In addition the application control feature can detect and block the usage of VPN apps.
• 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		On top of the predefined webfilter categories, admins may individual URLs by means of customizable block and allow lists. Furthermore, admins may also define custom categories.

filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		All changes on the configuration are logged accordingly for audit purposes.
● 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.		Currently not supported in the Barracuda Web Categorisation Microservice but we are working on a dedicated Contextual Filter specifically for AI generated content.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		In general we recommend a whitelist approach were everything except acceptable web categories and domains/URLs are blocked. A full list of available web filter categories is available here: https://campus.barracuda.com/doc/98216554/
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Barracuda Web Security Gateways can be centrally monitored and configured via the Barracuda Cloud Control. All Barracuda CloudGen Firewalls can be centrally managed via the Barracuda Control Center. The Barracuda SecureEdge Manager is the cloud-based central management piece that enables admins to easily configure Points-of-Entries (PoEs) and acceptable application usage and web policies.
● Identification - the filtering system should have the ability to identify users		Our solutions provide full user and group context via an integration with existing IdP (Identity Provider), Active Directory or LDAP systems.
● 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		The Barracuda Web Security Gateway, the Barracuda CloudGen Firewall as well as Barracuda SecureEdge provide a strong layer-7 application control to detect and enforce the usage of applications. In conjunction with TLS inspection our solutions allow for even deeper visibility, inspection and content filtering of web and non-web based applications.

clear about the capacity of their filtering system to manage content on mobile and web apps		
• Multiple language support – the ability for the system to manage relevant languages		Barracuda Networks has a world-wide deployment of filtering solutions and intelligence from this global footprint allows us to filter appropriately against content in multiple languages.
• 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)		Web filtering is provided at the network level.
• 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		For the Barracuda Web Security Gateway we provide the Web Security Agent that will route the web traffic through the Web Security Gateway for further inspection. For the Barracuda CloudGen Firewall as well as Barracuda SecureEdge the SecureEdge Access Agent extends security and policy compliance to any device on any platform.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Reporting of URLs for classification or re-classification can be done via the website barracudacentral.org or by simply contacting our worldwide support team.
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		Web logs are stored locally or can be streamed via syslog to external collectors or Azure Analytics
• Safe Search – the ability to enforce 'safe search' when using search engines		SafeSearch is fully supported. With the Barracuda Network Access Client and the SecureEdge Access Agent it is possible to enforce SafeSearch also for remote and off site users.

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

Web monitoring policies allow administrators to configure the generation events when certain content is searched on the Internet. You can select common categories from a list and also define

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

custom keywords in order to get notified about web content searched by users. As soon as web content defined as monitored is searched for, a notification event is generated and logged, and the admin receives a list containing the search terms looked for. This feature currently supports the following search engines: Google, Yahoo, Bing, YouTube, and DuckDuckGo.

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	Markus Lang
Position	Director Product Management, Network Security
Date	16.04.2024
Signature