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	WatchGuard Technologies, Inc.
Address	505 5th Ave South, Ste 500, Seattle, WA 98104
Contact details	mike.deichman@watchguard.com
Filtering System	WatchGuard Firebox
Date of assessment	September 18, 2023

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	🟩	Yes. WatchGuard is a proud and active member of the IWF.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	WatchGuard has actively monitored and self-tested against the IWF CAIC list for nearly 10 years.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	The Home Office police assessed list is regularly checked and incorporated by WatchGuard's web filtering partner Forcepoint, the provider of the database behind WatchGuard's URL Filtering capability.
● Confirm that filters for illegal content cannot be disabled by the school	🟨	Management of the device's configuration is flexible enough to meet the needs of varying organizations. Management UI can be secured with credentials controlled by the administrating body. WatchGuard's MFA solution, AuthPoint, can be implemented on the Management UI; further ensuring only authorized personnel are able to change or disable security settings.

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.	🟩	**Category: Intolerance** Filtering of sites that promote hate, violence, racism etc. are fully integrated and allows for reporting of inappropriate content. Application control beyond HTTP/S provides the ability to manage non-productive user activity such as access to chat/IM and inspect all SSL/TLS encrypted content regardless of port or protocol.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	**Category: Drugs** Specific filtering capabilities for Illegal categories especially web paraphernalia related to drug use. Ability to report on sites visited per user/group.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	**Category: Militancy and Extremist** Dedicated 'Militancy' and cover violence/hate and racism. Ability to apply blocking policies and report on user/group activity etc.
Gambling	Enables gambling	🟩	**Category: Gambling** Filtering of sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	**Category: Security** Watchguard offers a full suite of security services designed to break the malware cycle. These include filtering of access to know malware sites, file download restrictions, intrusion prevention, gateway antivirus, gateway anti-spyware, botnet filtering, Advanced Persistent Threat and integration with WatchGuard's endpoint security offerings.
Pornography	displays sexual acts or explicit images	🟩	**Category: Adult Content** Specific categories to filter access to pornography and adult content. Plus, ability to enforce Google/Bing safe search and YouTube restricted content on a per-policy basis.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	**Category: Illegal or Questionable; Information Technology** Filtering of access to known download sites hosting illegal copyrighted material. Application control over download tools such as BitTorrent, etc. Also, WatchGuard users are automatically granted application control/blocking of proxy bypass sites and tools to further limit risks.

Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	**Category: Violence** Filter on sites that feature or promote violence or bodily harm, including self-inflicted harm.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	**Category: Violence** Specific category for filtering sites that promote intolerance and illegal activities/skills as well as cult/occult sites. Again, further reporting and alert on site access, etc.

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

WatchGuard URL and content filtering solutions are based on firewall technology developed over more than 20 years. In addition, we proactively monitor our customer feedback to augment our internal capacity for rapid categorisation and blocking where our users can easily request a category change to augment our in-house blocking list. WatchGuard has been a recognised market leader in the provisioning of firewall appliances and UTM services as a Next Generation Firewall vendor.

By providing a fully integrated security solution, WatchGuard not only offers web filtering (HTTP and HTTPS) but also full content inspection of every packet traversing the firewall, regardless of port or protocol. This means, that in real-time, administrators can see exactly what is happening on their network and apply appropriate levels of control. In addition, bandwidth management and traffic prioritisation empower IT administrators to block certain applications, or features of an application, in real-time.

With the increased use of TLS encrypted traffic and data compression methods, it's still critical to be able to inspect and manage these popular transport mechanisms, regardless of port or protocol. WatchGuard solutions will decrypt SSL/TLS regardless of port/protocol and apply the same policies as for unencrypted traffic. Combined with comprehensive intrusion prevention, inspection of files of any size for 50M+ viruses (and increasing), botnet control and anti-malware, the solution provides industry leading security and safety at an affordable price for small office businesses to large, distributed education enterprises.

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.

The device-specific log file rolls over after a given storage value and typically doesn't contain more than a few hours' worth of data.

WatchGuard offers the capability for sites to host their own log servers on site where they can manage the retention as needed.

WatchGuard Fireboxes with the Total Security Suite or Basic Security Suite can utilize WatchGuard Cloud for reporting and log data. Devices with Total Security store logs in WatchGuard Cloud for three hundred sixty-five (365) days and devices with Basic Security store logs up to Ninety (90) days. Firebox configuration data is kept for up to 1 year of the device's last report to WatchGuard Cloud if it is taken offline.

WatchGuard Cloud is hosted in 3 separate regions: NA, EU and AP. Device, user and log data are tied to the specific WatchGuard account and remains within their respective region.

Removal of data can be requested.

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

All WatchGuard solutions are built on several critical foundations to deliver appropriate and effective security. By developing our own technology for over 20 years, WatchGuard has complete control over its products and service.

The technology architecture allows for granular policies to be designed and implemented. This ensures controls are applied to the appropriate users/groups and devices, avoiding over blocking (or under blocking!).

By undertaking our own threat research, analysing thousands of malware samples daily, analysing and categorising web content from 100,000's of sources means we are able to provide accurate intelligence for our solutions to use. That means, correctly categorised URLs, rapid development and deployment of malware signatures used by 100,000's of appliances worldwide. If a website needs to be assessed/reassessed quickly, our WatchGuard support engineers mobilise at a moment's notice to provide appropriate remediation and corrections on behalf of our customers.

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	🟩	Multiple policies can be applied based on AD group/OU membership etc. This allows policies to be developed an applied in the most appropriate way. Reporting based on AD group membership also available to ensure policies are being applied correctly.
● 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.	🟩	WatchGuard's Firebox has multiple network analysis and heuristic tools to detect proxy, and IT avoidance tools on the perimeter and network. WatchGuard's Application Control and IPS product work in tandem or singly to analyse network traffic directly and through side-channels to detect traffic patterns of unauthorized circumvention tools such as non-compliant VPNs or proxy services. In addition,

	🟩	WatchGuard’s endpoint client informs the Firebox of endpoint events that are designed to disrupt compliance and interrupt malicious behaviours against the host in real-time.
● 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 filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes	🟩	Policy development and implementation is performed via an intuitive UI. Management UI features an optional local teacher temporary override ability for blocked sites. Role based controls allow non-admin access to specific functions such as allowed/denied lists.
● 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.	🟧	Forcepoint, WatchGuard’s web filtering partner, scans pages as part of their URL categorization process. Once classified, the Watchguard Firebox makes use of the classification and actively scans for vulnerabilities and security risks but does not dynamically scan for URL category.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	WatchGuard has provided web filtering solutions for nearly 20 years to thousands of customers globally. The solution utilises in-house technology and research to ensure the highest levels of performance and accuracy. The WatchGuard Total Security Suite is responsible for dynamic/automated categorisation of sites, augmented by a skilled team of individuals to provide oversight and analysis of sites across multiple geographies and languages. Websites/URLs/subdomains/content delivery networks etc. are categorised into one or more categories as deemed appropriate. Website ratings can be checked via a public portal. WatchGuard is committed to constantly updating the database of malicious and unwanted websites against manual and automated analysis to ensure protection against known and rapidly occurring threats.

● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	WatchGuard Cloud provides central policy management, reporting, centralized logging and firewall template creation as well as executive reporting in addition to customized compliance reporting, providing a single ‘pane of glass’ for management and reporting needs.
● Identification - the filtering system should have the ability to identify users	🟩	Cohesive integration with AD and other external authentications systems provides identification of users on workstations, laptops, mobile devices etc. User/group information can be used for appropriate application of policy as well as reporting of user activity.
● 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 clear about the capacity of their filtering system to manage content on mobile and web apps	🟩	Sites/applications, regardless of client device, will be filtered and controlled as per policy design and implementation. Application traffic control empowers IT admins for control of specific mobile apps and inspect of SSL/TLS encrypted content regardless of port or protocol. In addition, Mobile VPN and explicit proxy options administered through the WatchGuard product line provides customizable filtering options through WatchGuard network appliances.
● Multiple language support – the ability for the system to manage relevant languages	🟩	Filtering and application control along with all other security services support multiple languages. Block, consent, authentication pages etc. can be customised to present in the desired 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)	🟩	WatchGuard proxy services provide inspection and filtering at the network level with no need to deploy endpoint agents. Every packet traversing the solution is inspected for millions of pieces of malware and intrusions regardless of port or protocol. The solution also provides for the inspection of all TLS/SSL encrypted traffic regardless of port or protocol.
● Remote devices – with many children and staff working remotely, the ability	🟩	Mobile User VPNs can be configured to force all traffic through the

for school owned devices to receive the same or equivalent filtering to that provided in school	🟩	WatchGuard Firebox where all of the available security services can be applied with the same principles as local users.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	WatchGuard Cloud provides extensive reporting against all web activity including, but not limited to, those blocked sites. Reporting includes user/group information, productive/unproductive, acceptable/unacceptable and full category-based reporting.
● Reports – the system offers clear historical information on the websites users have accessed or attempted to access	🟩	WatchGuard Fireboxes with the Total Security Suite or Basic Security Suite can utilize WatchGuard Cloud for reporting. Devices with Total Security can view detailed dashboards and reports up to thirty (30) days in the past.
● Safe Search – the ability to enforce 'safe search' when using search engines	🟩	Safe Search can be forced for major search engines and Youtube.

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

WatchGuard has actively engaged with the wider community for many years. Whether this is through organizations such as IWF or through directly working with schools, colleges and local communities to help develop an awareness and understanding of safeguarding issues. Safeguarding our communities is the cornerstone on which WatchGuard's leading technologies has continually innovated and built on. Prevention is better than the cure and education should underpin all efforts to keep everyone safer online.

[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	Mike Deichman
Position	Product Manager
Date	Aug 1, 2023
Signature	Mike Deichman