Appropriate Monitoring for Schools

May 2018

Monitoring 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 (e.g. 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. 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 monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	WatchGuard Technologies, Inc.
Address	505 5th Ave South, Ste 500, Seattle, WA 98104
Contact details	arthur.gordon@watchguard.com
Monitoring System	WatchGuard UTM Firewall
Date of assessment	July 03, 2018

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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		WatchGuard officially joined IWF in 2016; WatchGuard URL filtering provider has been IWF certified for over a decade, since 2003. In addition, the IWF list is integrated into WatchGuard's URL filtering solution daily after a 24 hour testing period.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		HMO police list is fully integrated into web filtering solution and updated monthly.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		**Category – e.g. Drugs, Extremist Groups, Hacking, Adult Content, Violence, Weapons and more** There are number of categories that block illegal content, activities and object, covered in the following categories. These categories can be both blocked and/or reported/alerted upon.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		**Category – Violence/Intolerance** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. These categories can be both blocked and/or reported/alerted upon.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		**Category – Adult Material; Sub-category: Adult Content** This category includes child abuse images and media that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is and the CAIC list is available at

			http://www.iwf.org.uk/. This combined with the ability to monitor HTTPS empowers the IT administrator to provide powerful blocking and reporting tools on attempted access to these websites.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		**Category – Intolerance** This category specifically includes websites that promote the identification of racial groups in degrading or hateful depictions. This category also includes websites promoting the superiority of any group at the expense of others. These categories can be both blocked and/or reported/alerted upon.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		**Category – Drugs** This category not only includes categorization on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, etc., but also sub categories related to • Abused Drugs • Marijuana • Nutrition • Prescribed Medications These categories can be both blocked and/or reported/alerted upon.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		**Category – Militancy and Extremist** This category specifically targets websites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs. These categories can be both blocked and/or reported/alerted upon.
Pornography	displays sexual acts or explicit images		**Category – Adult Material** This category is one of most extensive categories with a focus

			on explicit sexual content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. Sub categories include: • Adult Content • Lingerie and Swimsuit • Nudity • Sex • Sex Education These mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse are also categories that can be both blocked and/or reported/alerted upon.
Self Harm	promotes or displays deliberate self harm		**Category – Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. These categories can be both blocked and/or reported/alerted upon. This combined with the ability to monitor HTTPS and use Application Control to inspect communication channels such as Instant Messaging if permitted.
Suicide	Suggest the user is considering suicide		**Category - Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. These categories can be both blocked and/or reported/alerted upon. This combined with the ability to monitor HTTPS, allows IT admins to form an effective deterrent and monitoring solution to block violent and harmful content from students.
Violence	Displays or promotes the use of physical force intended to hurt or		**Category - Violence**

	kill		This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. These categories can be both blocked and/or reported/alerted upon.

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

WatchGuard web content filtering solutions are based on proxying technology developed over more than 20 years. Due to our depth of experience gleaned from developing our firewall technology in-house, WatchGuard has been recognised as a market leader in the provision of firewall, UTM/Next Generation Firewalls.

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

WatchGuard solutions are developed from a consistent and intentional feedback loop that we maintain with our customers. The architecture of WatchGuard solutions allows for granular filtering policies to be designed and implemented regardless of SSL layered protocols. This ensures controls are applied to the appropriate users/groups and devices - avoiding over blocking (or under blocking) - and any false positives or failed categorizations are easily received in our reporting/support portals.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access		Categories are not directly linked to age, instead the monitoring solution grants strong and flexible power to the IT administrator to decide which categories make sense for different age groups. WatchGuard's active directory integration allows admins to define policies by group, which could be defined by age, educational department, or any other distinction for purposes of granular monitoring and filtering policies.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Alert management is within the full ownership of the an organizational entity. There

		are notification settings concerning system health, database issues, etc. that can be configured for electronic based notices.
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		WatchGuard provides support for BYOD especially when implemented through WatchGuard secure Wi-Fi access points. With WatchGuard Wi-Fi and UTM tools, personal devices can be recognised as such and automatically assigned to a guest zone with a specific set of policies to avoid infections being passed into the school network, and to prevent access to internal systems. In addition, the WatchGuard firewall allows the ease and flexibility of explicit proxy configurations for school/enterprise owned mobile devices that are used for off-premise scenarios. Logging and reporting options are available based on flexibility for external or internal network environment locations of report server (s).
• Data retention –what data is stored, where and for how long		WatchGuard provides award-winning centralized reporting via Dimension, in which all web activity can be logged (generally to a centralised customer owned log server, where log retention is under the complete control of the user or to a third-party infrastructure provider). The data stored includes user id (if users are individually authenticated via RADIUS or AD integration), URL visited, the ID of the security device which handled the

		transaction, as well as low-level addressing information and a timestamp.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		WatchGuard offers flexible monitoring solutions that can be deployed on devices or in clientless deployment scenarios. WatchGuard provides monitoring solutions through Mobile VPN solutions as well as clientless explicit proxy solutions for select mobile devices that do not require WatchGuard client installations. WatchGuard also supports the native VPN clients of iOS and Windows devices to promote alternative clientless VPN deployments.
• Flexibility – schools ability to amend (add or remove) keywords easily		The WatchGuard URL filtering and web categorization services provides ease of search by categorization as well as aggregate search term logging. Basic keyword filtering is available in the UTM DLP solution. In addition, scripts are available to generate reports based on search terms.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		WatchGuard contains several management platforms to accelerate deployment. In addition to our RapidDeploy feature that allows for remote templated firewall configuration, our WatchGuard Management Server allows for the ability to deploy central policies through a single management pane.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		In general, if a user is blocked after accessing a web site which belongs to a blocked category, a customisable block page will

		be displayed which can contain an explanation for the block, as well as information on whom to contact for more information, or a link to a support website.
• Multiple language support – the ability for the system to manage relevant languages?		The WatchGuard web filtering solution is multilingual, both in the automated rating system, as well as for the human web categorization team which contains skills in all major languages to allow for detailed verification of page ratings.
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		Any blocked access will generate a log message, which may also generate an alert. Such alerts may be generated for every blocked rule. The alerts can then be sent by several means including email, SNMP traps.
• Reporting – how alerts are recorded within the system?		As explained above, all detections of forbidden or suspicious access will be logged in the WatchGuard UTM device and Dimension product. Additionally, WatchGuard products provide flexible rules for log management including retention times, executive and technical summarization of logs in user-configurable dashboards.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

WatchGuard works closely with the education sector and multiple authoritative compliance bodies to determine the optimal mix of technology tools and policies to enable conducive educational environments for students. We continue to work closely with UK authorities, authoritative certification bodies (Friendly WiFi, IWF etc.) and educational partners to refine our products according to KCSIE policy development and the needs of our educational users.

MONITORING 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	Arthur Gordon
Position	Senior Product Manager
Date	07/02/2018
Signature