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	Exa Networks
Address	100 Bolton Road, Bradford, BD1 4DE
Contact details	mark.cowgill@exa.net.uk or 0345 1451234
Filtering System	SurfProtect Quantum
Date of assessment	6th October 2021

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		Exa have been full members of the IWF for over fifteen years
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		And the CAIC URL List is included as standard on SurfProtect Quantum and cannot be deactivated
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, the CTIRU assessed list is included with SurfProtect Quantum and cannot be deactivated

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.		Our standard education profile (default) for Education would block the category "Intolerance and Hate" which includes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Our standard education profile (default) for Education would block the category "Drugs" which includes sites that displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Our standard education profile (default) for Education would block the category "Extremism" which includes sites that promotes terrorism and terrorist ideologies, violence or intolerance
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Our standard education profile (default) for Education would block the category "Malware" which includes sites that promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

Pornography	displays sexual acts or explicit images		Our standard education profile (default) for Education would block the category "Pornography/Adult Content" which includes sites that displays sexual acts or explicit image
Piracy and copyright theft	includes illegal provision of copyrighted material		Our standard education profile (default) for Education would block the category "Piracy & Copyright Theft" which includes sites that includes illegal provision of copyrighted material. We also integrate the Intellectual Property list into SurfProtect, which cannot be deactivated.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Our standard education profile (default) for Education would block the category "Self Harm" which includes sites that promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	Displays or promotes the use of physical force intended to hurt or kill		Our standard education profile (default) for Education would block the category "Violence" which includes sites that Displays or promotes the use of physical force intended to hurt or kill

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

Using Exa's own propriety categorisation system, which has been continually developed since SurfProtect first launched in 2005, there are more than 50 separate categories, all of which are continually assessed automatically, and recatagorise where appropriate

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 .

By default, we retain the log files and analytical information for organisations to access in real time. Organisations also can download the full log files to import into third party analytical software. This information is kept on the system and fully accessible for at least 90 days.
Schools who require log files and data to be retain longer have an option for service upgrades for this.

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

SurfProtect Quantum has been designed from the ground up entirely by Exa Networks, to put the control of access back in the hands of the organisations using the service, whilst being mindful of things such as the IWF List, and legislation around the Prevent Duty. For any category where a site does not fall under the IWF List, Prevent, CTIRU or the Intellectual Property List, they can recatagorise any site as all filtering is by its definition, subjective depending on who is using the service. SurfProtect Quantum allows for a unlimited number of profiles to be set up for each organisation site, all of which can have different permissions on what is and is not available, and fully integrates into Active Directories for this to be done on a per user or group level if required.

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		SurfProtect Quantum has age policy based rules if the organisation provides them via group information on Active Directory. A policy can be created For instance for 10 year olds to have access to all acceptable sites (as judged by the school) but have Social Media excluded, if the user group had <Name_Year5> passed through and the policy was based on that. The per user, or per group filtering policies are very powerful and allow the customer to define exactly what is suitable for users of groups on an individual level dependent on age and role.
• 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 category “Proxy or VPN” which is blocked by default for schools on the standard profile, is designed to stop access to sites or functionality, which are used to circumvent the system. If we are also providing or managing the firewall system for the school we add

		additional complimentary rules and application control in too.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		SurfProtect Quantum gives the school full administrative ability to permit of deny, or recatagorise specific content as required, in real-time.
• 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		SurfProtect Quantums classification systems and in built dynamic filtering looks at far more than just a domain or IP address. This includes contextually analysis of the text on a page, but also the forward and backward links to where traffic is going to or from, in order to make a more informed classification decision.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Our default polices that are applied with our service are published within our SurfProtect & Safeguarding documentation. We also regularly publish further information or guidance on our blog.exa.net.uk
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		SurfProtect Quantum allows for multi-site or group management, including pushing out of policies, shared subscriptions services (for filtering profiles), central management and oversight.
• Identification - the filtering system should have the ability to identify users		SurfProtect Quantum ties into Active Directory and identifies usage on a per user and IP based system, with full time stamp information. This is available directly from the portal.
• 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		SurfProtect Quantum runs in both Transparent mode and Proxy Mode, dependent on the customer requirement.

via mobile and app technologies (beyond typical web browser delivered content)		Users can be authenticated using a captive portal, and a certificate can be installed from the captive page for HTTPS filtering. All none HTTPS is filtering transparently if the customer is using Exa's connectivity and via Proxy if external. VPNs can also be set up by the school on mobile or tablet devices if the end users is using a different network (such as Home user or 4G) to force the connection through the schools filtered service. We also provide a Chrome plugin to connect back to the active directory integration with SurfProtect and provide the same level of filtering, and reporting on any connection (such as working from home)
● Multiple language support – the ability for the system to manage relevant languages		SurfProtect Quantum supports multiple languages at a filtering level
● 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)		SurfProtect Quantum is a cloud based service and does not require any software to be installed on user devices, with the exception of a HTTPS/SSL certificate for HTTPS filtering. The service is fully run within Exa's own network infrastructure, and entirely in the UK.
● 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		SurfProtect Quantum runs in both Transparent mode and Proxy Mode, dependent on the customer requirement. Users can be authenticated using a captive portal, and a certificate can be installed from the captive page for HTTPS filtering. All none HTTPS is filtering transparently if the customer is using Exa's connectivity and via Proxy if external.

		VPNs can also be set up by the school on mobile or tablet devices if the end users is using a different network (such as Home user or 4G) to force the connection through the schools filtered service. We also provide a Chrome plugin to connect back to the active directory integration with SurfProtect and provide the same level of filtering, and reporting on any connection (such as working from home
• Reporting mechanism – the ability to report inappropriate content for access or blocking		SurfProtect Quantum has built in real time analytical information. If a organisation believes something is incorrect catagorised they can force a change to their own filtering, report it to Exa via our Help Desk by email or phone (for us to assess centrally), or if the matter is illegal in nature for us to in turn contact the relevant authorities.
• Reports – the system offers clear historical information on the websites visited by your users		SurfProtect Quantum includes real-time reporting and analytical information which allows for detailed reports on user or IP address based activity. We have also introduced real-time alerts which notify designated users/administrators of any access to banned sites or categories. This includes Pornography, Hate, Suicide, Prevent and others.

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

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

We further support schools through the Exa Foundation, which includes completely free on-site or virtual CPD for Teachers, Students and Parents across a range of subject lessons, including E-Safety. We also offer our Protect & Connect package for schools, which includes the connectivity, filtering, Securus Monitoring, Firewall, Router Management & Anti-Virus for a complete protection package.

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	Mark Cowgill
Position	Co-Founder & Director
Date	7th October 2021
Signature	M Cowgill