Appropriate Filtering for Education settings

June 2016

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*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated 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 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	Orbis Education Network (Orbis ICT Partnerships) *Includes the East Sussex Education Network and the Brighton & Hove Education Network*
Address	County Hall, Lewes, East Sussex. BN7 1UE
Contact details	itd@orbis.services
Filtering System	Smoothwall
Date of assessment	8 October 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	

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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

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		Smoothwall, our web content filtering partner, are a member of the Internet Watch Foundation and implement the IWF CAIC list
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Smoothwall implement the IWF CAIC list of domains and URLs. Smoothwall also use a number of search terms and phrases provided by IWF and their members. They perform self-certification tests daily to ensure that IWF content is always blocked
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

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.		Smoothwall provides an 'Intolerance' category which covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Smoothwall provides a Drugs category which covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered

			by the 'Alcohol and Tobacco' category.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Smoothwall provides a 'Terrorism' category which contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Smoothwall provides a 'Malware and Hacking' category which contains sites known to promote or contain trojans or spyware. The category also covers malware distribution sites and sites which aim to steal personal details by impersonating other trusted sites. Sites which aim to bypass filtering are covered by the 'Web Proxies' category which contains both Domains/URLs as well as dynamic content rules.
Pornography	displays sexual acts or explicit images		Smoothwall provides a 'Pornography' category which contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a static list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.
Piracy and copyright theft	includes illegal provision of copyrighted material		Smoothwall provide a 'Piracy and Copyright Infringement' category which contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Smoothwall proves a 'Self Harm' category which contains sites relating to self-harm, suicide and eating disorders. The category

			excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Smoothwall provides a 'Violence' category which contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content.

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

As well as the categories listed above, Smoothwall provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and 'Non-Pornographic Nudity' through to 'News', 'Sport' and 'Online Games'.

Smoothwall uses a wide variety of techniques in order to identify and categorise content. All categories use a static list of both URLs and domains, with the majority of categories also using search terms, weighted phrases and regular expressions to identify content on the fly.

Smoothwall have an in-house categorisation team which are responsible for maintaining and updating the blocklist which is released to customers on a daily basis; ensuring that schools are always protected from the latest threats.

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

What is and is not blocked depends primarily on the policies specified by the customer. However, the underlying categorisation is based very little on URLs, and focuses mostly on the content of pages. This uses a weighting mechanism rather than automatically categorising a site as "pornography" for only one mention of "porn" on a page. This weighting mechanism allows sites to be more accurately classified and filtered upon, without unduly restricting access. Furthermore, while these same underlying categories are also used for identifying sites for the purpose of the Safeguarding suite of tools, a site may be allowed according to the filtering policy, but still be flagged as a potential issue in Safeguarding reports. This means a school can provide access to a large degree of the internet, while also keeping an eye on content accessed by pupils. With this degree of visibility and awareness, pupils can be educated rather than merely ring-fenced.

The OEN Service allows for individual schools to determine their own policies even when using the central network filtering servers. A default set of school rules were identified for all schools from the outset based upon the skills and experience of the team at Smoothwall and in liaison with a selection of East Sussex and Brighton & Hove Schools. We also ensure that that key areas, such as Internet Watch Foundation filtering, are applied across the system and cannot be overridden

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		Smoothwall can integrate with various directory services and through doing so, apply filtering based on the user group. As long as the directory structure reflects the needed criteria (such as age and role), this is fully achievable. The OEN Smoothwall central service also provides different filtering policies that can be configured to different groups based upon proxy server settings in instances where directory configuration is not available
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Smoothwall offers our schools easy to use policy management, with a range of shortcut features designed to simplify making simple configuration changes, such as a dashboard feature to allow someone to quickly block or allow a site. Control over basic settings can be delegated to school users with our service desk support team offering schools the ability to generate more granular control as needed as a part of the service
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		The publishing guides are currently being rewritten to reflect our most recent updates within the product.
• Identification - the filtering system should have the ability to identify users		Smoothwall can integrate with various directory services (including AD and Google) and through doing so, apply filtering based on

		the user group. We then have a number of different mechanisms to ensure users are identified, such as a logon page, Kerberos, a Chrome plug-in and others. This can be done across the wider OEN network
● Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		Both for local and remote filtering Smoothwall are able to filter all http and https connections from a client, this is not limited to browser traffic and includes mobile and app connections.
● Multiple language support – the ability for the system to manage relevant languages		Smoothwall performs dynamic content analysis in a variety of languages in order to identify content and to ensure schools can monitor or block said content as required
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		The OEN Smoothwall service does not make and reliance on software and is applied at the network level
● Reporting mechanism – the ability to report inappropriate content for access or blocking		There is the availability to enable a reporting function on the block page, allowing users to report inappropriately blocked content. There is no dedicated mechanism to enable the users to advise administrators of inappropriately allowed content. But there is also a mechanism for customers to report back to Smoothwall on both inappropriate allows and blocked content.
● Reports – the system offers clear historical information on the websites visited by your users		The system offers very comprehensive controls over how much data is retained, it is then made available through a large and powerful reporting tool.

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*".[3]

Please note below opportunities to support schools (and other settings) in this regard

As well as providing ad-hoc advice to customers, Smoothwall have recently embarked on a campaign of workshops with customers discussing safeguarding. We have shown off the specific suite of reports and alerting tools we offer to support this, as well as including a number of specialist guest speakers to help provide the full context. This has been extremely well received, and has significantly contributed to the shared understanding of safeguarding within the community of Smoothwall customers. In addition the Orbis Education Network through the Orbis ICT Partnership team provide a full managed support service and are always happy to talk to our schools to ensure that the systems are working as they require. We are also investigating other options in how we can assist schools meet their requirements in other aspects of online safety.

[3] 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	Richard May
Position	Business Development Manager, Orbis IT & Digital (East Sussex County Council and Brighton & Hove City Council)
Date	8 October 2018
Signature