Appropriate Filtering for Education settings

September 2019

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. 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."

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	Smoothwall
Address	Avalon, 1 Savannah Way, Leeds, LS10 1AB, United Kingdom
Contact details	0870 1999 500
Filtering System	Smoothwall Web Filter
Date of assessment	21/10/2019

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, Smoothwall 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 URL 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. We perform self-certification tests daily to ensure that IWF content is always blocked through a Smoothwall.
• 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		As well as providing a level of protection against externally created malware, Smoothwall provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.
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 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 provides 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 list of both URLs and domains, with the majority of categories also using search terms, content-based rulesets, and regular expressions to identify content on the fly.

Smoothwall have an in-house Digital Safety Team which are responsible for maintaining and updating site categorisation rules which are released to customers on at least a daily basis; ensuring that schools are always protected from the latest threats

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

Data retention is offered as a control to the customer. As the data controller it is right that they are able to choose the data retention period most appropriate to their users. The retention period is only hard limited by the amount of diskspace the customer has and the volume of logs.

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 highly granular, and assesses the content of pages. This uses an intelligent rules-based mechanism rather than automatically categorising a site as "pornography" for only one mention of "porn" on a page. This intelligence 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 Smoothwall's 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 proportion 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 being ring-fenced.

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 integrates with a wide variety of directories (e.g. Microsoft AD, Google Directory) allowing filtering to be set appropriately at group and user level.
• 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.		Smoothwall maintains an extensive rules database for detecting circumvention activity. VPNs should also be blocked by a firewall – Smoothwall's optional Firewall uses Layer 7 analysis to identify nonweb VPN traffic. DNS-over-HTTP may be blocked by preventing access to these types of DNS service, however DoH would NOT allow a user to bypass the filter control as we do not use DNS for filtering.
• 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 has a full range of policy tools available, allowing School users to easily make policy changes, test a site against current policy or simply quickly allow or block a site.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Smoothwall maintains a "blocklist policy document" which includes clear criteria on what should and should not be in each category. This is available on request.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Smoothwall allows for multi-tenant deployments, where a central unit controls policy and reporting. Delegated access is available. Smoothwall can work in a cluster as well as a standalone unit.
• Identification - the filtering system should have the ability to identify users		Smoothwall offers a wide range of techniques for identifying users – including negotiate authentication, login pages, and RADIUS

		compatibility, as well as a number of custom options.
• 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)		Any app content delivered via HTTPS (not necessarily through a web browser) can be blocked and inspected by Smoothwall, assuming the app permits this. In addition, Smoothwall's optional firewall module can identify and block many other types of app.
• Multiple language support – the ability for the system to manage relevant languages		Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.
• Network level - filtering should be applied at 'network level' i.e, not reliant on any software on user devices		Smoothwall is a network level filter.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Smoothwall provides the ability to report overblocked content to the administrator. Uncategorised content (which is possibly "underblocked") is automatically fed back to Smoothwall and will subsequently be appropriately categorized.
• Reports – the system offers clear historical information on the websites visited by your users		Smoothwall offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device. Logs are retained to customer preference.

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

As well as providing ad-hoc advice to customers, Smoothwall has recently embarked on a campaign of workshops with customers discussing digital 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 digital safeguarding within the community of Smoothwall customers.

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	Douglas Hanley
Position	Chief Technical officer
Date	21/10/2019
Signature