Appropriate Filtering for Education settings

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by
SWGfL Childnet IWF

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	DNSFilter, Inc
Address	80 M Street SE, Suite 100, Washington, DC 20003
Contact details	Sales: sales@dnsfilter.com, this cert: ken@dnsfilter.com
Filtering System	DNSFilter
Date of assessment	Nov 27, 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	🟩	
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	
● Confirm that filters for illegal content cannot be disabled by the school	🟨	The solution is administered by customer.

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.	🟩	
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	
Gambling	Enables gambling	🟩	
Malware / Hacking	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	🟩	
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	This is part of our terrorism and hate category.
Violence	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

We allow the network operator to select categories. Additionally, we have in house ML that constantly updates our database, which is call Webshrinker

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.

DNS traffic request logs are viewable within the web based dashboard for 90 days

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

We work on our Webshrinker ML to ensure categorizations remain accurate. We also allow for customer feedback directly in our dashboard, which is constantly monitored.

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	🟨	We don't make this judgement. It is up to the customer to pick what is appropriate for 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.	🟩	We offer best deployment practices and the ability to block proxy and VPN services
● 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	🟩	Fully configurable via our web based dashboard
● 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.	🟨	Our filter operates at the DNS level and dynamically filters against categories set by the administrator.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Fully configurable via our web based dashboard

● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Fully configurable via our web based dashboard
● Identification - the filtering system should have the ability to identify users	🟩	We can do this through on site proxy, or through roaming client deployment
● 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	🟩	We can block entire applications
● Multiple language support – the ability for the system to manage relevant languages	🟩	We offer block pages in many languages
● 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)	🟩	Available in dashboard
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school	🟩	Need to install Remote Client on individual devices
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Available in dashboard
● Reports – the system offers clear historical information on the websites users have accessed or attempted to access	🟩	Available in dashboard
● Safe Search – the ability to enforce 'safe search' when using search engines	🟩	Available in dashboard

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

We believe DNS is a great way to filer, because it allows the filtering to happen across all devices on the network, as well as the ability to extend protection to the home, in 1:1 deployment instances. However, it is extremely important, in our opinion, that the customer follows our best practices for deployment. This involves additional settings on your router and/or firewall to ensure circumventions opportunities are at a minimum.

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

Finally, the IT administrator should take advantage of our dashboard and ensure to constantly review reporting to identify any unusual activity or attempts on the network.

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	Lauren Romer
Position	General Counsel
Date	12/13/2023
Signature	DocuSigned by: Lauren Romer A44EDCF305764A1...