

Appropriate Filtering for Education settings

June 2018

Filtering Provider Checklist Responses

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	DNSFilter, Inc.
Address	1440 G Street NW, Washington, D.C. 20005, United States
Contact details	For sales: sales@dnsfilter.com, For this certification: Ken Carnesi - ken@dnsfilter.com
Filtering System	DNSFilter
Date of assessment	February 6, 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
<ul style="list-style-type: none"> Are IWF members 		
<ul style="list-style-type: none"> and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list) 		
<ul style="list-style-type: none"> Integrate the '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.		
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		
Extremism	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		
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, but we are working to split it out separately.
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 AI that constantly updates our database. This product is called Webshrinker.

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 AI 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
<ul style="list-style-type: none"> Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role 		We don't make this judgement. The customer should pick what's appropriate for the age.
<ul style="list-style-type: none"> Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services 		We offer best deployment practices and the ability to block proxy and VPN services.
<ul style="list-style-type: none"> Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content 		Fully configurable via our web based dashboard.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		Fully configurable via our web based dashboard.
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		We can do this through on site proxy, or through roaming client deployment.
<ul style="list-style-type: none"> 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) 		We can block entire applications, if that's what you mean.
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		We offer block pages in many languages.
<ul style="list-style-type: none"> Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices 		Available in dashboard.
<ul style="list-style-type: none"> Reporting mechanism – the ability to report inappropriate content for access or blocking 		Available in dashboard.
<ul style="list-style-type: none"> Reports – the system offers clear historical information on the websites visited by your users 		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 filter, 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's 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 circumvention opportunities are at a minimum.

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.

¹ <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	Kenneth B. Carnesi, Jr.
Position	CEO
Date	February 6, 2019
Signature	