

# 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](mailto: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	SafeDNS
Address	901 North Pitt Street Suite #325 Alexandria VA 22314
Contact details	mail@safedns.com, +1 571 421 2990 (outside US)
Filtering System	SafeDNS Cloud Filtering Service
Date of assessment	April 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
<ul style="list-style-type: none"> <li>Are IWF members</li> </ul>		Since 2015
<ul style="list-style-type: none"> <li>and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)</li> </ul>		SafeDNS includes the contents of the IWF CAIC list into a dedicated filtering category, named 'Child Sexual Abuse (IWF)' for blocking these images
<ul style="list-style-type: none"> <li>Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'</li> </ul>		To block terrorism-related content, SafeDNS adds the list of sites compiled by Counter Terrorism Internet Referral Unit/CTIRU (run by the Metropolitan Police, UK) to a filtering category, named 'Hate & Discrimination'

## 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.		The SafeDNS filtering service has a dedicated filtering category, 'Hate & Discrimination' for blocking specifically this type of content
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		The SafeDNS filtering service has a dedicated filtering category, named 'Drugs' for blocking specifically this type of content
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		All terrorism-related content is included into the 'Hate & Discrimination' category
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		The SafeDNS filtering service has a dedicated filtering category, named 'Virus Propagation' for blocking malware and virus propagating sites
Pornography	displays sexual acts or explicit images		The SafeDNS filtering service has a dedicated filtering category, named 'Pornography & Sexuality' for blocking specifically this type of content
Piracy and copyright theft	includes illegal provision of copyrighted material		The SafeDNS filtering service has dedicated filtering category, named 'Torrents & P2P' for blocking specifically this type of content

Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)self harm (including suicide and eating disorders)		
Violence	Displays or promotes the use of physical force intended to hurt or kill		For blocking child abuse content SafeDNS has 2 filtering categories, dedicated to such material. One category contains illegal resources from the IWF CAIC list, the other category – illegal resources from a list compiled by the Canadian Centre for Child Protection, as part of its Project Arachnid

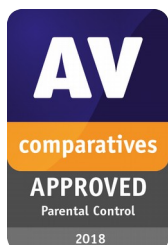
This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

SafeDNS provides a cloud-based web filtering service, tailored to the needs of educational institutions – from kindergartens to elementary, secondary and high schools, colleges, universities and libraries ([safedns.com/safe-internet-for-educational-institutions](https://safedns.com/safe-internet-for-educational-institutions)). To start filtering the internet with SafeDNS, users should change the network settings on the devices they want to have the filtering on – a server/firewall/WiFi router/endpoints (desktops/laptops, tablets, smartphones, gaming consoles, smart TV-sets, etc.)

Once the user deploys the SafeDNS filtering service on a network, each DNS query of users of this network is directed to company’s DNS servers for analysis from the point of view of a content category the requested site belongs to. If it belongs to a category, allowed on this network, the DNS query is successfully resolved into the IP of the requested site. If anybody tries to access a site from a blocked content category, then the service responses with the block page IP address and the network users are going to see a service block page instead of the requested site.

The SafeDNS distributed network of 13 filtering servers, located all over the world, allows us to fast resolve DNS queries with no added latency. SafeDNS is in the top 3 of the world's fastest DNS filtering services ([dnsperf.com/#!/dns-resolvers](https://dnsperf.com/#!/dns-resolvers)).

With SafeDNS you can block the entire site, no matter how many web pages it contains. Thus, SafeDNS prevents any possible harm done to its users from porn and explicit sites, child and adult sexual abuse content, malicious and phishing sites, online time wasters – in a word, any unwanted and inappropriate content.



Since 2015 the SafeDNS ability to efficiently filter out porn and adult sites has been proved multiple times during rigorous annual tests and reviews by AV-Comparatives, a world-known test lab. As a result SafeDNS has for 4 consecutive years been acknowledged Approved Parental Control Product by the lab.

According to the 2018 test results, SafeDNS blocks near-perfect 98.3% of requests to adult content ([av-comparatives.org/news/parental-control-certification-test-2018](https://av-comparatives.org/news/parental-control-certification-test-2018)). For all the 4 years of testing SafeDNS has returned zero false positives. That is why company's users face no overblocking issues.

To enable customers to easily block child sexual abuse images and videos, SafeDNS has 2 filtering categories, fully dedicated to such content. One of these 2 categories contains illegal resources from the IWF CAIC list, which SafeDNS receives as IWF Member.



The other category contains illegal resources from a list compiled by the Canadian Centre for Child Protection, as part of its Project Arachnid ([protectchildren.ca/en/programs-and-initiatives/project-arachnid](http://protectchildren.ca/en/programs-and-initiatives/project-arachnid)).

SafeDNS supports this project as the company works to safeguard web surfers from gross stuff online as well as contribute to preventing distribution and sharing child abuse material online and prevent re-victimization of survivors.

SafeDNS has a separate category, named 'German Youth Protection', for blocking sites from a list compiled by Germany's Federal Department for media harmful to young persons/BPJM. In the list Department includes resources that provoke violence, crime and racial hatred.



SafeDNS is Approved Partner of Friendly WiFi, a UK government-initiated safety certification for public WiFi. This means that the SafeDNS filtering solutions are recommended by Friendly WiFi for use by public WiFi owners and providers to secure their wireless networks from cyber threats and inappropriate content.

The technological foundation of SafeDNS is the company's own web categorization database with over 105M sites in it, distributed into 60 content categories. The database is exceptionally precise as SafeDNS uses AI and machine learning to automatically categorize internet resources and add them to the dynamically updated database.

SafeDNS provides multiple features and options to adapt its filtering service to each user's specific requirements. One of the most important ones is the SafeDNS service blocks HTTP/unencrypted sites as well as HTTPS/encrypted ones. The latter now comprises over 70% of all the existing websites and the number of the HTTPS sites grows rapidly as encryption improves users security.

SafeDNS allows users to make per policy exceptions from filtering rules – just add the necessary sites to a white list of the chosen filtering policy. To 'whitelist' a site makes it freely accessible to the network users with a specific filtering policy, no matter which content category the whitelisted site belongs to.

'Blacklisting' works the other way around. A site, blacklisted for users with a specific filtering policy, will always be blocked, its content category notwithstanding.

A filtering schedule feature allows the SafeDNS customers to switch filtering policies for their network users during the day.

With SafeDNS, an educational institution/library can have a fully personalized block page per each filtering policy to let its network users know why a particular site is blocked and whom to contact to have it unblocked. All of the enumerated service features are needed to further personalize the filtering and adapt it to educational institutions' needs.

The company provides agent software, SafeDNS Agent for PCs. Agent comes in handy for installing, connecting to and managing the filtering service on Windows-based computers. Agent is adapted to be used in large organizations with hundreds of PCs to filter the internet on.

On its website SafeDNS provides multiple user guides on how to set up the filtering service on different kinds of web-connected devices ([safedns.com/en/guide](https://safedns.com/en/guide)). The complete SafeDNS Service Guide is available at: [safedns.com/en/guides/guide-main](https://safedns.com/en/guides/guide-main).

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

Since 2015 SafeDNS has annually been tested and reviewed by AV-Comparatives, a world-known test lab. For all the 4 years of testing SafeDNS has returned zero false positives. That is why company's users face no overblocking issues.

## Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>		The SafeDNS filtering service can be adapted to the user's exact needs – to filter the internet differently for small children, pre-teens, teens, and adults
<ul style="list-style-type: none"> <li>Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services</li> </ul>		SafeDNS has a dedicated filtering category, named 'Proxies & Anonymizers' for blocking such means of circumventing the filtering
<ul style="list-style-type: none"> <li>Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>		The SafeDNS filtering service is managed via an online management panel/Service Dashboard where the service users create and change their filtering settings. With user credentials (the login and password) Dashboard is available 24/7 from anywhere on the internet
<ul style="list-style-type: none"> <li>Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>		The SafeDNS service users create their own filtering policies with an individual set of filtering rules per each policy by choosing which categories of content to block or allow out of the 60 existing categories.
<ul style="list-style-type: none"> <li>Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard</li> </ul>		SafeDNS provides the ability for deployment of central policy and central dashboard

<ul style="list-style-type: none"> <li>• Identification - the filtering system should have the ability to identify users</li> </ul>		SafeDNS identifies users by determining unique browsers on the service block page
<ul style="list-style-type: none"> <li>• 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)</li> </ul>		For filtering the internet on mobile devices SafeDNS recommends users to set the filtering service on WiFi routers of the educational institution. A SafeDNS app for filtering the internet on Android devices will be released next month
<ul style="list-style-type: none"> <li>• Multiple language support – the ability for the system to manage relevant languages</li> </ul>		SafeDNS Service Dashboard is available in Arabic, Brazilian Portuguese, English, French, German, Italian, Spanish, Swedish, Turkish, Urdu
<ul style="list-style-type: none"> <li>• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices</li> </ul>		To have the filtering network-wide, set SafeDNS up on a piece of networking hardware – server/ firewall/ WiFi router
<ul style="list-style-type: none"> <li>• Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		In per-policy internet usage stats SafeDNS provides, filtering service admins can see if there have been attempts to access inappropriate content
<ul style="list-style-type: none"> <li>• Reports – the system offers clear historical information on the websites visited by your users</li> </ul>		The SafeDNS filtering service provides detailed internet usage stats per filtering policy

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*”.<sup>1</sup>

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

SafeDNS can provide schools and other educational institutions as well as students’ parents with tips (PDF docs) on keeping students safe online at places of learning and at home. SafeDNS Team can assist the school staff (IT, administrators, teachers) and parents in learning more about the SafeDNS filtering service, ways to manage it via Dashboard by holding webinars and providing service guides.

To extend protection of the students against inappropriate and unwanted web content, their parents can also use SafeDNS at home. For home users the SafeDNS filtering service is available for a small fee of \$19,95 per year (on Safe@Home Plan: [safedns.com/safe-internet-at-home](https://safedns.com/safe-internet-at-home)) or completely free – on Free plan (with a limited functionality). Both service plans apply for protecting unlimited number of family’s devices.

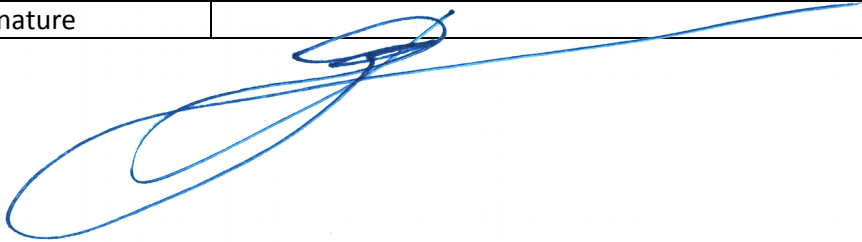
<sup>1</sup> <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

## 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	Dmitry Vostretsov
Position	CEO
Date	April 10, 2019
Signature	

A handwritten signature in blue ink, appearing to be 'Dmitry Vostretsov', is written over the signature field of the table and extends horizontally across the page.