# Appropriate Filtering for Education settings

**June 2021**

## 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*" and they "should be doing all that they reasonably can to limit children's exposure to the above 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."

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 | SafeDNS |
| --- | --- |
| Address | 901 North Pitt Street, Suite 325 Alexandria, VA 22314 |
| Contact details | sales@safedns.com |
| Filtering System | DNS based |
| Date of assessment | 15-Dec-21 |

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. | <span style="color:green">■</span> |
| 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. | <span style="color:orange">■</span> |

.

## 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 | | https://www.safedns.com/en/news/safedns-iwf-membership/ |
| ● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) | | https://www.safedns.com/en/news/safedns-iwf-membership/ |
| ● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | https://www.safedns.com/en/news/safedns-included-into-uk-safer-internet-centre-list-of-filtering-providers/ |

## 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. | | SafeDNS doesn't promote 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 | | SafeDNS doesn't promote drugs or anything related to drugs, SafeDNS is blocking by default all content related to drugs |
| Extremism | promotes terrorism and terrorist ideologies, violence or intolerance | | SafeDNS blocks any content related to violence and doesn't promote any terrorism or violence related content. |
| Malware / Hacking | promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content | | SafeDNS is blocking Malware/hacking by default. |
| Pornography | displays sexual acts or explicit images | | SafeDNS doesn't promote pornography and offers a pornography category that can be blocked in the users dashboard. |
| Piracy and copyright theft | includes illegal provision of copyrighted material | | SafeDNS doesn't use any copyrighted materials. |
| Self Harm | promotes or displays deliberate self harm (including suicide and eating disorders) | | SafeDNS doesn't promote anything related to the Self Harm content. |

| | | | |
|---|---|---|---|
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | SafeDNS blocks Violence content by default. |

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

> SafeDNS developed it's own categorization system to classify any type of websites into 61 category. There are special tools to gather and analyze data based on ML, AI and user behavior.

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 .

> According to the GDPR rules the users' statistics are saved for up to 1 year.

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

> Globally there are special tools and classificators that help analyze the content on any website. Special algorithms identify the inappropriate content.

## 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 | | The filter can be configured on individual devices for granular protection. Using the option "Schedule" makes the filter more flexible. |
| ● 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 do have bypass prevention recommendation and we can filter some VPN services (DNS based), but we do not support DoH or DNSSEC yet. |
| ● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content | | Yes, the SafeDNS will help you with that - https://safedns.com/cabinet |
| ● 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.  For example, being able to contextually | | SafeDNS cloud is a web filter based on DNS only. It can not block IP or URL. |

| | | |
|---|---|---|
| analyse text on a page and dynamically filter | | |
| ● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking | | We have over 60 categories - https://www.safedns.com/en/categories/ |
| ● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard | | The dashboard can be managed by any appropriate person with the login and the password from any place. It's possible to create multiple filtering policies under one account and assign them to different sites (locations) |
| ● Identification - the filtering system should have the ability to identify users | | Created users can be identified by username, policy ID. |
| ● 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) | | Currently, we can block DNS requests only. But the iOS and Android filtering apps are coming soon, they will cover this goal. |
| ● Multiple language support – the ability for the system to manage relevant languages | | Interface language can be changed on the dashboard. |
| ● 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) | | The filter can be configured on the router to filter all devices connected to its network or you can install the SafeDNS agent on individual devices for more granular protection. |
| ● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school | | It is possible to filter devices outside the school network. You need to install the SafeDNS agent |
| ● Reporting mechanism – the ability to report inappropriate content for access or blocking | | We do not have a reporting mechanism that notifies you when some one is trying to reach a blocked website, but we do have detailed statistics section that |

| | | shows all of your requests, their status and time. |
|---|---|---|
| ● Reports – the system offers clear historical information on the websites visited by your users | | Yes, the statistics section is comprehensive and allows to receive monthly reports. |

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

SafeDNS believes that all students and staff should no worry about nothing else other than searching for knowledge in the internet,  where all they need to do is to connect to their WiFi and SafeDNS will drive their internet traffic from there by filtering the unwanted and harmful content. Surely SafeDNS is offering unique pricing draft for schools, SafeDNS also helped many schools who were under the budget by giving them free license.

---

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

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 | Xenia Hayes |
|---|---|
| Position | Head of Marketing |
| Date | 12.21.2021 |
| Signature | |