

Appropriate Filtering for Education settings



May 2023



Filtering Provider Checklist Responses

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 | Netsweeper UK |
| Address | Suite 125-126 Pure Offices, 4100 Park Approach Thorpe Park, Leeds United Kingdom LS15 8GB |
| Contact details | Nick Levey |
| Filtering System | Netsweeper |
| Date of assessment | 10/06/2023 |

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 |
|---|--------|---|
| <ul style="list-style-type: none"> Are IWF members | | We are member of the IWF |
| <ul style="list-style-type: none"> and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) | | We implement the IWF and other lists to block child |
| <ul style="list-style-type: none"> Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | We incorporate this list |
| <ul style="list-style-type: none"> Confirm that filters for illegal content cannot be disabled by the school | | These are pushed down as immutable categories |

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. | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Drugs / Substance abuse | displays or promotes the illegal use of drugs or substances | | Netsweeper uses dynamic content analysis to categories, this and many other content types. |
| Extremism | promotes terrorism and terrorist ideologies, violence or intolerance | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Gambling | Enables gambling | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Malware / Hacking | promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Pornography | displays sexual acts or explicit images | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Piracy and copyright theft | includes illegal provision of copyrighted material | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |

| | | | |
|-----------|--|--|---|
| Self Harm | promotes or displays deliberate self harm (including suicide and eating disorders) | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | Netsweeper uses dynamic content analysis to categories , this and many other content types. |

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

Netsweeper uses a tiered filtering methodology based around dynamic content analysis to ensure we can accurately categories these and many other categories. Netsweeper uses AI based technology to perform dynamic categorisation of over 90 categories in 47 languages. Netsweeper also has inhouse digital safety and categorisation teams working continuously at improve our categorisation algorithms and lists.

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.

Storage duration can be defined from our customer, theoretically any given storage requirement length could be catered for.

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

Market leading dynamic content analysis as well as easy to manage unblocking and recategorization tools ensure high levels of accuracy and ensure overblocking is not a problem

Filtering System Features

How does the filtering system meet the following principles:

| Principle | Rating | Explanation |
|---|--------|---|
| <ul style="list-style-type: none"> Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff | | Netsweeper allows for differentiated filtering based on different user types. For example students may receive differentiated filtering based on age. Vulnerable users may have certain categories blocked that are not blocked for other uses. |
| <ul style="list-style-type: none"> Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, | | Netsweeper used advanced technology to detect and prevent |

| | | |
|--|--|--|
| specifically VPN, proxy services and DNS over HTTPS. | | attempts to circumvent the system. |
| <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. 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 | | All changes made to the system are logged and auditable by the school. The schools are able to administer their own content filtering. |
| <ul style="list-style-type: none"> 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. | | Netsweeper provides on the fly categorisation based on the content and context of text and links that appear on the page. |
| <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 | | We have a stated filtering methodology |
| <ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard | | Netsweeper has full multitenancy |
| <ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users | | Users can be identified by various methodologies including but not limited to azure, AD , google |
| <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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps | | Netsweeper is capable of filtering all device based content including content delivered via apps. |
| <ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages | | Netsweeper performs dynamic filtering in 47 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 whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure) | | Filtering can be performed at the Network level |
| <ul style="list-style-type: none"> 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 | | Netsweeper can deliver identical filtering to the schools devices onsite and offsite |

| | | |
|---|--|---|
| <ul style="list-style-type: none"> ● Reporting mechanism – the ability to report inappropriate content for access or blocking | | We offer both reports and live alerts, with both premade templates and the ability to make custom reports |
| <ul style="list-style-type: none"> ● Reports – the system offers clear historical information on the websites users have accessed or attempted to access | | We offer both reports and live alerts, with both premade templates and the ability to make custom reports |
| <ul style="list-style-type: none"> ● Safe Search – the ability to enforce ‘safe search’ when using search engines | | Safe search can be enforced |

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

Netsweeper offers a range of products in the monitoring space. As well as offering numerous training packages in the safeguarding space.

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 | Nick Levey |
| Position | Regional Director |
| Date | 10/06/23 |
| Signature |  |