Appropriate Filtering for Education settings

June 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	Coconnect
Address	Harbour House, Hamilton Road, Cosham, Portsmouth, Hampshire, PO6 4PU
Contact details	Email: hello@coconnect.co.uk | Telephone: 02392 322 522
Filtering System	Netsweeper, Smoothwall and FortiGate
Date of assessment	June 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	🟨	Netsweeper and Smoothwall are all long standing members of IWF.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	Netsweeper and Smoothwall all block access to illegal Child Abuse Images by actively implementing the IWF CAIC list of domains and URLs.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Netsweeper and Smoothwall block all terrorist content as per the Home Office's terrorism blocklist. It offers unmatched global protection against terrorist and extremist content.
● Confirm that filters for illegal content cannot be disabled by the school	🟩	All illegal content categories are locked at a system level. Schools cannot disable these filters.

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 and Smoothwall have categories that identify websites/content that are intentionally offensive by being discriminatory about race, ethnicity, nationality, gender, sexual orientation, religion, disability or profession.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Netsweeper and Smoothwall block websites/content that feature or encourage illegal drug activities such as the sale, manufacture, distribution or use of drugs and drug paraphernalia. Informational sites featuring information about drugs (such as descriptions, negative effects etc) are not blocked.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Netsweeper and Smoothwall categorise and block any websites/content under the ‘police assessed list of unlawful terrorist content’. This covers categories including extremism, hate speech, criminal skills, terrorism, and weapons.
Gambling	Enables gambling	🟩	Netsweeper and Smoothwall blocks sites that encourage or provide information on gambling (including sites that encourage risking of money on games, contests, and other events. Sites that are strategic or promote cheating are also blocked. Sites for gambling addiction support are not blocked.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	Netsweeper and Smoothwall block websites that are associated with malware and hacking. This includes malware, infected hosts, phishing, viruses, and adware.
Pornography	displays sexual acts or explicit images	🟩	Netsweeper and Smoothwall block websites/content that contain pornographic images, videos, and text. Websites/content that depict full or partial nudity are also blocked.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Netsweeper and Smoothwall block websites that illegally provide copyrighted material or peer-to-peer software.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Netsweeper and Smoothwall block websites/content relating to self-harm, suicide and eating disorders. Websites providing medical information or support are not blocked.

Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Netsweeper and Smoothwall block websites/content depicting or advocating violence against people and animals. This includes torture, self-inflicted harm, mutilation, suicide, death, gore and injuries.

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 accurately categorise these and many other categories. Their AI based technology performs dynamic categorisation of over 90 categories in 47 languages. Netsweeper also has inhouse digital safety and categorisation teams working continuously at improve their categorisation algorithms and lists.

Smoothwall provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and 'Non-Pornographic Nudity' through to 'News', 'Sport' and 'Online Games'. They use a wide variety of techniques to identify and categorise content. All categories use a list of both URLs and domains (with most categories using search terms, content-based rulesets, and regular expressions to identify content quickly). Smoothwall has an in-house Digital Safety Team which is responsible for maintaining and updating the site categorisation rules which are released to customers on at least a daily basis.

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.

We keep all logfile data for 1 year, as per our retention policy.

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

To ensure over blocking isn't a problem, we regularly review our blocked categories, URLs, and keywords to make sure key educational content isn't blocked. It's very easy for us to unblock and recategorise any blocked categories, URLs, and keywords at the request of the school (so long as it doesn't go against the inappropriate content outlined above.

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	🟩	Netsweeper and Smoothwall integrates with existing directory systems (such as Microsoft AD, Azure AD and Google Directory) so filtering

	🟩	can be set appropriately at a group and user level. Assigning users to groups means they'll receive appropriate filtering based on their age, vulnerability, or risk of harm.
● 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.	🟩	Netsweeper and Smoothwall use advanced technology to detect and prevent any attempts made to circumvent the system.
● 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	🟩	Coconnect configures different roles for users. This allows schools to control and maintain the filters and reports themselves. All changes made either by Coconnect or the school are logged for a full audit trail.
● 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 and Smoothwall analyse and categorise content in real time.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Netsweeper and Smoothwall have their own filtering rationale that includes clear criteria on what should be included (and what should not be) in each category. Care is taken not to over block.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Under Netsweeper's filtering, Coconnect provides a single pane of glass service where policies can be shared across multiple schools. This works in conjunction with reporting, providing hierarchical views for Multi Academy Trusts and federated schools. Under Smoothwall, each school has access to their own interface for reporting

	🟩	and to make adjustments to filtering policies.
● Identification - the filtering system should have the ability to identify users	🟩	Netsweeper and Smoothwall integrates with existing directory systems (such as Microsoft AD, Azure AD and Google Directory) so different users can be identified and appropriate filtering set accordingly.
● 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	🟩	Coconnect utilises Layer 7 application inspection for mobile and application technologies. Layer 7 application filtering is delivered via with Netsweeper and Smoothwall firewalls (depending on deployment method selected by the school).
● Multiple language support – the ability for the system to manage relevant languages	🟩	Netsweeper and Smoothwall have extensive directories for multiple languages, as well as human web filtering teams with fluency in multiple 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)	🟩	Netsweeper and Smoothwall can apply filtering on a network level, so all devices are covered.
● 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 and Smoothwall can apply filtering down to a device level to cover devices on the school network even if it's offsite.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Schools can immediately block/allow access so long as they have an admin role. We also work with designated contacts at the school, to make sure they can report inappropriate content to us. This can be done through our online portal, telephone, or email.
● Reports – the system offers clear historical information on the websites users have accessed or attempted to access	🟩	Netsweeper and Smoothwall have their own reporting engines. These allow schools

	🟩	to see various reports, data, and alerts
● Safe Search – the ability to enforce 'safe search' when using search engines	🟩	Safe Search can be applied for set user groups at the request of the school.

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.

Coconnect focuses on safeguarding and online safety and has a number of different measures in place to educate and support schools in keeping students safe. We provide online guidance for safeguarding through webinars, blog posts, and social media, and are currently producing guides and videos to assist in self-learning. We can also tailor custom messages displayed to students when they try and access blocked content. This means that rather than just blocking a website/page/content, we can educate students and advise where they can get help if they need it.

Netsweeper and Smoothwall also offer a range of additional products for filtering and monitoring that schools can choose to add to enhance their safeguarding solutions.

[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	Shayne Grove
Position	Director of Education Services
Date	26/06/2023
Signature	