UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet IWF

Appropriate Filtering for Education settings

May 2025

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	Smoothwall by Qoria
Address	2 Whitehall Quay, Leeds, LS1 4HR
Contact details	https://smoothwall.com/contact-us
Filtering System	Smoothwall Filter
Date of assessment	7 Jan 2026

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	🟩	Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update	🟩	Smoothwall implements the IWF CAIC list of domains and URLs and update it at least daily. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self-certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
● Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).	🟩	The IWF rules cannot be disabled, however school leaders should be aware that system administrators may be able to entirely bypass filtering by altering the network configuration (e.g. by removing the content filter entirely).

Describing how, their system manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.	🟩	In addition to the IWF list content, the Child Abuse category also includes words, phrases and search terms to dynamically identify and block such content.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.	🟩	These types of actions are more commonly identified and flagged to the school with a separate monitoring product, such as Smoothwall Monitor, which analyses conversations and interactions. However web content promoting or advising

		🟩	techniques on how to achieve this will be blocked by the filter.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.	🟩	This is categorised and blocked according to the defined school policy under both the Violence and Pornography categories. In addition, the optional real-time image and video filtering add-on will analyse and blur media on all websites for such content.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.	🟩	This is categorised and blocked according to the defined school policy under both the Violence and Pornography categories. In addition, the optional real-time image and video filtering add-on will analyse and blur media on all websites for such content.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.	🟩	This is categorised and blocked according to the defined school policy under either of the Hacking and Criminal Activity categories.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.	🟩	This is categorised and blocked according to the defined school policy under the Intolerance category.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.	🟩	This is categorised and blocked according to the defined school policy under the Violence category.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.	🟩	This is categorised and blocked according to the defined school policy under the Criminal Activity category.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.	🟩	This is categorised and blocked according to the defined school policy under the Self Harm category.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.	🟩	This is categorised and blocked according to the defined school policy under the Pornography category. In addition, the optional real-time image and video filtering add-on will analyse and blur media on all websites for such content.

selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.	🟩	This is categorised and blocked according to the defined school policy under either the Drugs or Weapons categories.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.	🟩	This is categorised and blocked according to the defined school policy under the Pornography category.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.	🟩	This is categorised and blocked according to the defined school policy under the Terrorism category.

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
Gambling	Enables gambling	🟩	This is categorised and blocked according to the defined school policy under the Gambling category.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010	🟩	This is categorised and blocked according to the defined school policy under the Intolerance category.
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.	🟩	This is categorised and blocked according to the defined school policy under either of the Violence, Drugs or Adult Mixed Content categories.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	This is categorised and blocked according to the defined school policy under either of the Hacking, Malware and Phishing, or Web Proxies categories.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining	🟩	By using the News category, schools can control the sources that students have access to in their policy to only allow access to trusted media outlets.

	trust in factual information or institutions	🟩	
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	This is categorised and blocked according to the defined school policy under the Piracy category.
Pornography	displays sexual acts or explicit images	🟩	This is categorised and blocked according to the defined school policy under the Pornography category. In addition, the optional real-time image and video filtering add-on will analyse and blur media on all websites for such content.
Self Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide	🟩	This is categorised and blocked according to the defined school policy under the Self Harm category.
Violence Against Women and Girls (VAWG)	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.	🟩	This is categorised and blocked according to the defined school policy under either of the Violence or Intolerance categories.

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

As well as the categories listed above, Smoothwall Filter provides filtering and reporting for hundreds of other categories including standard categorisations such as ‘News’, ‘Sport’ and ‘Online Games’, application signatures covering a wide variety of apps and tools that schools may wish to allow or block, and education-specific categories such as ‘Educational Games’, ‘Sex Education’ and ‘Translation’.

Smoothwall Filter uses a wide variety of techniques in order to identify and categorise content. All categories use lists of both URLs and domains, with the majority of categories also using search terms, content-based rulesets, and regular expressions to identify content dynamically in real time. 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 - ensuring that schools are always protected from the latest risks.

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.

Retention policies when using on-premise reporting are set by customer preference (and limited by size of disk). Smoothwall will assist customers in specifying the correct hardware for their desired retention. Customers are encouraged to discuss with Smoothwall their retention requirements when using Cloud Reporting, for which the standard retention is 3 months. All loglines are identified by the user’s directory username unless an on-premise device is not configured with authentication.

Data is either held on the customer’s on-premise appliance or in Smoothwall by Qoria’s cloud systems. The highest standards of security and privacy are used to ensure the safety of this data, including SOC2 accreditation, as described at https://qoria.com/trust

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

What is and is not blocked depends primarily on the policies specified by the customer. However, the underlying categorisation is highly granular, and assesses the content of pages in real time. This uses an intelligent rules-based mechanism rather than automatically categorising a site as “pornography” for only one mention of “porn” on a page. This intelligence allows sites to be more accurately classified and filtered upon, without unduly restricting access. Furthermore, while these same underlying categories are also used for identifying sites for the purpose of Smoothwall’s Safeguarding suite of tools, a site may be allowed according to the filtering policy, but still be flagged as a potential issue in Safeguarding reports. This means a school can provide access to a large proportion of the internet, while also keeping an eye on content accessed by pupils. With this degree of visibility and awareness, pupils can be educated rather than merely ring-fenced.

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	🟩	Smoothwall Filter integrates with a wide variety of directories (e.g.Microsoft AD, Azure AD/Entra ID, Google Directory) allowing filtering to be set appropriately at group and use level. It is also possible to combine user group with location (eg outside school)
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services, DNS over HTTPS and ECH.	🟩	Smoothwall maintains an extensive rules database for detecting circumvention activity. VPNs must also be blocked by a firewall – Smoothwall's optional Firewall uses Layer 7 analysis to identify non-web VPN traffic. On-device filtering adds an additional layer of protection as this occurs within the browser, so is able to see the same content that the user sees, regardless of the underlying network transport (therefore fully able to filter content received via DoH, ECH and even VPN).
● 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	🟩	Smoothwall Filter has a full range of policy tools available, allowing School users to easily make policy changes, test a site against current policy or simply quickly allow or block a site. All changes made through the cloud filter portal are recorded in an audit trail.
● Contextual Content Filters – in addition to URL or IP based filtering, Schools should understand the extent to which (http and https) content is dynamically analysed as it is streamed to the user and blocked. This would	🟩	All web content (HTTP and HTTPS) is analysed in real time and dynamically categorised by Smoothwall Filter. The content, context

include AI or user generated content, for example, being able to contextually analyse text and dynamically filter the content produced (for example ChatGPT). For schools' strategy or policy that allows the use of AI or user generated content, understanding the technical limitations of the system, such as whether it supports real-time filtering, is important.	🟩	and construction of each page is assessed in real time to build a dynamic categorisation of the content, rather than simply relying on the URL.
● Deployment – filtering systems can be deployed in a variety (and combination) of ways (eg on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations	🟩	Smoothwall Filter can be deployed as a network level filtering appliance, or as an on-device filter which is controlled from the cloud. We recommend that where possible all student machines are protected with an on-device filter as this offers the highest level of protection and is able to filter in real time regardless of the network environment (at school, at home, using DoH, ECH, VPN etc). However, schools may choose to augment this with a network-level appliance for BYOD and Guest traffic where it is impractical to implement an on-device filter.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses over blocking	🟩	Smoothwall maintains a "blocklist policy document" which includes clear criteria on what should and should not be in each category. This is available on request
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Smoothwall products allow for multi-tenant deployments, with a single MAT or local authority customer account having tenants for the schools within it. Policy control and reporting can be safely delegated, such as to a school administrator or DSL, while the MAT/LA can still have visibility over all their schools as well as enforce policy that cannot be

	🟩	overridden by the school-level administrators for compliance and peace of mind.
● Identification - the filtering system should have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.	🟩	Smoothwall Filter offers a wide range of techniques for identifying users – including negotiate authentication, login pages and RADIUS compatibility, as well as obtaining user and group information from Active Directory, Entra ID (Azure AD) and Google Workspace.
● 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 capability of their filtering system to manage content on mobile and web apps and any configuration or component requirements to achieve this	🟩	Any app content delivered via HTTP/HTTPS (not necessarily through a web browser) can be blocked and inspected by Smoothwall's on-premise network appliance, assuming the app permits this. In addition, Smoothwall's optional firewall module can identify and block many other types of non-web app. Filtering agents are also available for Android and iOS to provide on-device analysis including outside the school premises.
● Multiple language support – the ability for the system to manage relevant languages	🟩	Smoothwall's combined categorisations include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.
● 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	🟩	The on-device filter provides filtering regardless of the physical location of the device, and co-ordinates policy and reporting via the Cloud.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Smoothwall provides the ability to report overblocked content to the administrator. Uncategorised content (which is possibly

	🟩	“underblocked”) is automatically fed back to Smoothwall and will subsequently be appropriately categorised.
● Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access	🟩	Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device.
● Safe Search – the ability to enforce ‘safe search’ when using search engines	🟩	Smoothwall offers forced safesearch on all major search engines, social media sites and some niche providers.
● Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity	🟩	Smoothwall’s Monitor product integrates with popular case management platforms.

How does your filtering system manage access to Generative AI technologies (e.g. ChatGPT, image generators, writing assistants)?

In your response, please describe whether and how your system identifies, categorises, or blocks Generative AI tools; how access can be controlled based on age, risk, or educational need; any limitations in filtering AI-generated content—particularly where such content is embedded within other platforms or applications; and what support or configuration guidance you offer to schools to help them align with the UK Safer Internet Centre’s Appropriate Filtering Definitions and relevant national safeguarding frameworks.

Smoothwall Filter provides two key categories for controlling AI usage: AI Tools and Unsafe AI Chat. These allow schools to permit or deny access broadly to all AI tools, as well as restrict those known to have unsafe practices such as allowing risky and harmful conversations.

In addition, application categories are available for all major AI platforms (including ChatGPT, Google Gemini, Microsoft Copilot), allowing schools to make their own safety, security and privacy risk assessments. For example, if a school determines Google Gemini to be their sole acceptable platform, they can block the AI Tools category whilst allowing only the Google Gemini category.

All controls can be set at a granular level based on age, role or educational need - such as only for staff, specific year groups, or individual students. This allows schools to align access policies with their risk assessments and curriculum requirements. All usage is logged and available for reporting to identify which tools are being used and by whom.

Smoothwall Filter can dynamically analyse content produced by AI tools. The optional real-time image and video analysis add-on identifies and blurs pornographic, gory or risqué content, including AI-generated media. Text responses from AI tools can also be partially analysed, however the rapidly changing nature of AI tools and the ways in which they deliver content means this shouldn't be solely relied upon as a safety net.

We provide configuration guidance aligned with the UK Safer Internet Centre's Appropriate Filtering Definitions and DfE safeguarding frameworks. We recommend schools:

- Assess the risks of AI tools against their safeguarding policies
- Only allow access to those known to be safe, secure and private
- Use monitoring tools such as Smoothwall Monitor to provide contextual analysis of conversations with these tools, including text captures and screenshots reviewed by human moderators
- Regularly review and adjust policies as the AI landscape evolves.

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

As part of the wider Qoria group, Smoothwall offers a wide range of products and support for schools, including best-in-class Monitoring, Record Management, Classroom Management and Student Wellbeing tools. Additionally Smoothwall offers training and resources to promote safety in UK schools, including a school branded "hub" for parents and students.

[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	Rob Faulkner
Position	VP Product
Date	7 Jan 2026
Signature	