

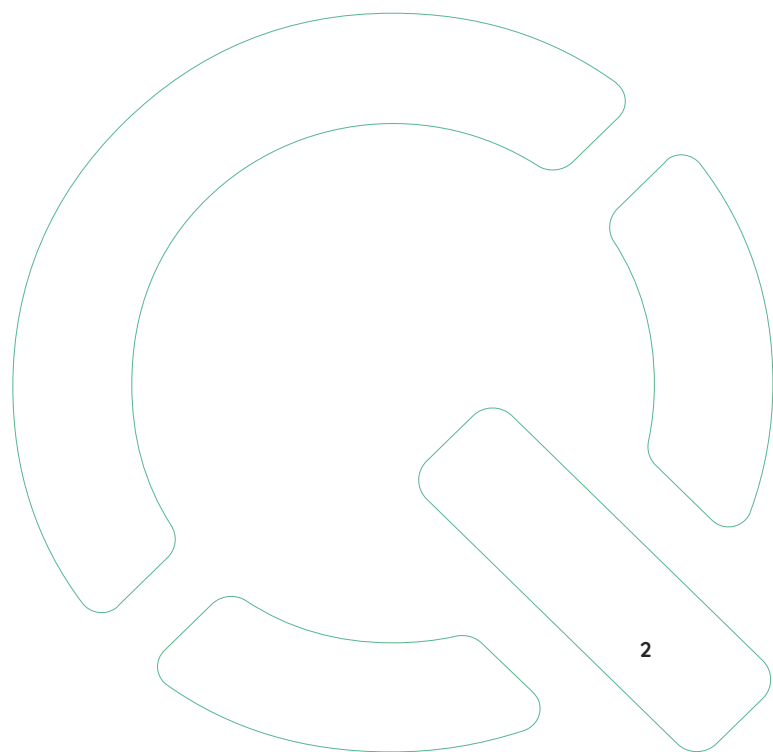


A Complete Guide to Real-Time, Content-Aware Web Filtering

Essential reading for: ITs, DSLs, headteachers, governors, school leaders and anyone with a responsibility or interest in digital safeguarding.

Contents

Introduction	03
Web Filtering in UK Education	04
What is Content-Aware Web Filtering?	04
What is Real-Time Web Filtering?	06
Combined to Achieve Unparalleled Web Filtering	07
No compromise on safety or learning	07
Meet and exceed statutory guidance	07
Keep Pace with Emerging Digital Threats	08
AI content	08
Subdomains	08
Anonymous proxies	09
Hacked websites	09
Real-time, Content-Aware Filtering: A Powerful Combination	10



Introduction

In the world of web filtering, one type of filter sits a class above the rest: real-time, content-aware web filters. They are the only web filters capable of establishing appropriate standards of online safety as outlined by KCSIE and other statutory guidance.



This guide breaks down what makes these filters so powerful, and how their application can help schools, colleges and MATs take their digital safeguarding to the next level.

Real-time, content-aware web filters utilise cutting edge technology to perform a nuanced, targeted method of web filtering.

The result is an online environment in which students can freely explore the internet while enjoying a high level of protection from harmful content.

“They are the only web filters capable of establishing appropriate standards of online safety as outlined by KCSIE and other statutory guidance.”

Web Filtering in UK Education

Now that online learning is a staple of the student experience, all UK schools are required to have “appropriate filtering systems in place” (KCSIE, 2024).

Web filters are designed to keep pupils away from dangerous parts of the internet and shield them from inappropriate or harmful material. At the same time, they need to ensure that students still have enough

access to online content to achieve a productive learning experience and develop key skills.

There are a **range of web filters used in education**, but few of them are able to meet these important criteria - today’s digital landscape requires a highly sophisticated approach.

What is Content-Aware Web Filtering?

Where basic tools like DNS or URL filters rely on pre-existing blocklists of sites and web pages to decide which content to restrict, content-aware filters assess the actual content of a web page.

The web address is just the beginning. A content-aware filter will analyse words and media, as well as the context and construction of the web page a user is attempting to access. This gives it the power to detect harmful or unwanted content, even when it is hidden using anonymous proxies, when it is user-generated content as part of a larger site (e.g. Reddit or YouTube), or when it is on a previously unseen, or very new site.

Assessing the content, context and construction of a web page is also known as granular filtering, and it significantly reduces overblocking (when a filter blocks pages with potential educational value) and underblocking (when a filter fails to restrict harmful content).

Unfortunately, due to the potentially ambiguous nature of the term “content filter”, the label is sometimes applied to simple URL web filters. Only filters that inspect the content of web pages can be considered content-aware.

Context alone plays a significant role in potential safeguarding incidents. For example, there’s a big difference between a search for “how to build a bomb” and one for “how to build a project around the atom bomb”.



100%

Real-time filters base decisions on instant assessments of the present version of web pages to effectively filter content.

What is Real-Time Web Filtering?

Real-time web filtering means that pages are analysed for harmful content at the point of request. In other words, assessment takes place and permission is granted or denied while the user is navigating the internet.

This technique ensures that there is no delay between harmful content going live and the filter blocking it. Not all content-aware filters possess real-time analysis capabilities. Some may grant access to web pages based on analysis conducted days, weeks or even months ago. As dangerous content often moves between different domains, turning previously harmless pages into potential safeguarding threats, this puts students in a vulnerable position.

Forums and social media feeds are customised for individual users, meaning what one person sees when they visit the homepage will be different to the content presented to another user. Non-real-time filters are unable to protect students from malicious content that appears on such pages, as the technology can only rely on analysis of previous iterations to judge whether to block them or not.

As a result, schools may be forced to block entire sites like Reddit and YouTube, which contain many forms of exciting, educational content.

100% real-time filters base decisions on instant assessments of the present version of web pages to effectively filter content. This approach is the only way to ensure safety for children when dealing with a constantly-evolving ecosystem like the internet.



Combined to Achieve Unparalleled Web Filtering

No compromise on safety or learning

A filter that combines real-time and content-aware capabilities empowers schools to let their students explore the internet with confidence and security. Without the level of protection this technology provides, educators may find themselves having to restrict large amounts of online content (some of which has educational benefits) just to keep their pupils safe.

Real-time, content-aware web filters can also be programmed to establish appropriate learning environments for different age groups. Flexible controls offer the ability to give older students access to more complex or challenging content, which they need to be exposed to in order to develop skills like critical thinking. These pupils will soon be adults with full access to the internet, so it's important that they are trained to use it wisely and with care.

“Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.”

Department for Education

Meet and exceed statutory guidance

Keeping Children Safe In Education states that establishing what constitutes appropriate filtering is “a matter for individual schools and colleges”, as settings have varying requirements. The document directs schools to two sets of guidelines, both of which reference a level of filtering only achieved by real-time, content-aware web filters.

The first is the **Filtering and Monitoring Standards for Schools and Colleges** from the Department for Education. Detailing the standards schools should already be meeting, it asserts: “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.” This delicate balance is almost impossible to achieve with URL or non-real-time, content-aware web filters.

Further confirming this, the second resource referenced by KCSIE 2024 is the **Appropriate Filtering Guide** from the UK Safer Internet Centre (UK SIC). Included in its list of principles required from a web filtering system is “Contextual Content Filters” - another term for content-aware filters. In 2024, UK SIC **updated their definitions of appropriate filtering**, directing schools to consider “the extent to which content is analysed as it is streamed in real-time to the user and blocked.” It states that contextual content filters need real-time capabilities to address potential threats like “AI generated content”, which is rapidly growing online.

Keep Pace with Emerging Digital Threats

Technology moves fast, and nowhere is this more apparent than online. Schools, colleges and MATs require web filters that can keep up with the changing demands of digital safeguarding. Dynamic real-time, content-aware web filtering is up to the task, as can be seen below when applied to four emerging digital trends.



AI content



Subdomains



Anonymous proxies



Hacked websites



Digital threat: AI content

Potential issue: Generative AI can produce vast amounts of inappropriate content in seconds. Unlike search engines, what a user types into generative AI tools does not necessarily appear in the URL, meaning web filters that can only analyse domains and URLs are unable to identify the category of content being consumed. Content-aware filters relying on analysis of past versions of pages face a similar issue.

The solution: Real-time, content-aware filters inspect the content on the page that is being requested by the user at that specific moment. This means it can accurately assess the nature of the material being sought or produced and respond accordingly.



Digital threat: Subdomains

Potential issue: The use of subdomains (a prefix added to a domain, used to direct users to a separate section of a site) means that inappropriate content can be found on URLs that schools may not otherwise want to block. For example, Google Sites hosts a range of custom-created apps, many of which are not suitable for students. URL filters would have to block all access to Google to prevent pupils using such apps.

The solution: Real-time, content-aware web filtering's granular approach enables organisations to block inappropriate Google pages, while still allowing network users to access other Google sites for their learning and development opportunities.



Digital threat: Anonymous proxies

Potential issue: A common tactic of school filter avoidance is the use of anonymous proxies - tools that provide users with harmless looking URLs to disguise their activity on pages that would otherwise be restricted. This deception can even fool content-aware web filters, as URLs used as decoys may have previously hosted harmless content, and without an up-to-date analysis available, the filter will act as if this is still the case.

The solution: By analysing the construction of web pages, real-time, content-aware filters can identify the software used by anonymous proxies, and block them immediately, even if it is the first time that particular version has been used.



Digital threat: Hacked websites

Potential issue: It is common for poorly maintained sites to be hijacked by hackers who update them to include inappropriate content and/or links to harmful content. An example of this is a tourism site for an English city which now includes a number of links to pornographic sites. The URL gives no indication to the harmful links within, and a majority of the content is harmless, meaning it could easily be deemed safe by URL and non-real-time filters.

The solution: A real-time, content-aware web filter assesses the content, context and construction of entire pages, ensuring that no malicious content slips under the radar. As it inspects the current version of a website, even pages that were previously safe will be blocked as soon as they are hacked.



Real-Time, Content-Aware Filtering: A Powerful Combination

The internet is a dynamic, ever-changing landscape. Allowing students to navigate this environment with the protection of a URL or non-real-time web filter is the equivalent of sending them into a storm with a broken umbrella.

Only real-time, content-aware web filters can offer:

- Instant analysis of all web-based content
- Enhanced cyber security by protecting both networks and users
- Flexibility and peace of mind for School leaders, DSLs and IT teams
- A rich online educational experience for students

Want to understand the impact real-time, content-aware web filtering could have in your setting?

Learn more about Smoothwall Filter or request a demo by contacting enquiries@smoothwall.com.

We're waiting to help.



smoothwall[®]
by Qoria

Smoothwall is the leading provider of digital safeguarding solutions in UK education. For more information, visit our website or get in touch with our team of experts.

Web: www.smoothwall.com

Tel: +44 (0)800 047 8191

Email: enquiries@smoothwall.com

Qoria

Smoothwall is part of Qoria, a global technology company, dedicated to keeping children safe and well in their digital lives. We harness the power of connection to close the gaps that children fall through, and to seamlessly support them on all sides - at school, at home and everywhere in between.

Find out more

www.qoria.com