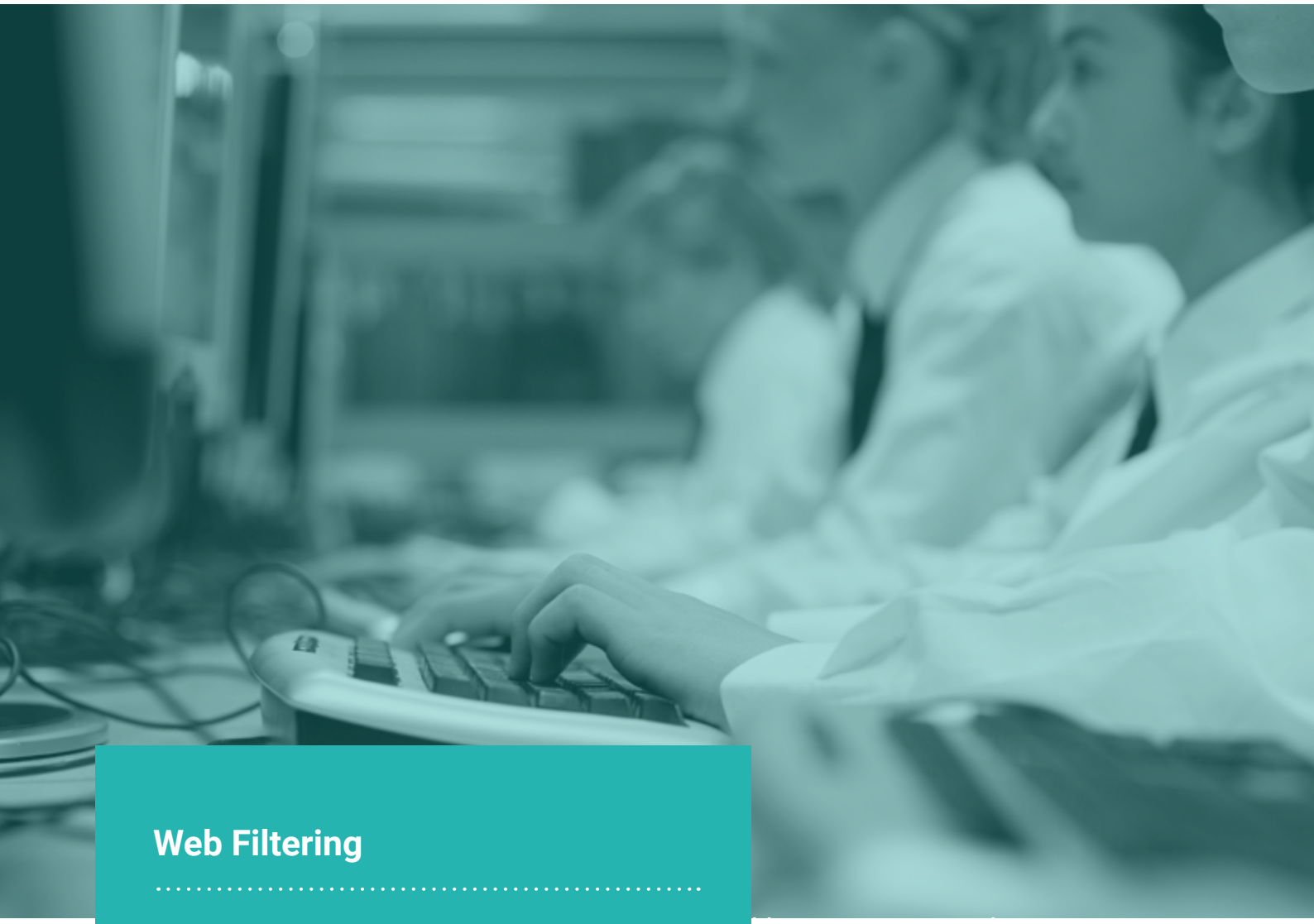
Smoothwall for Education

Whitepaper



Web Filtering

The 7 Imperatives of Web Filtering in an Independent School

Essential reading for:

IT Leaders in independent schools in the UK and around the world.

smoothwall®

smoothwall.com

Contents

Whitepaper

About This Document

All web filters are not created equally - so how do we tell the difference between basic web filters and those that are suitable for a premium education environment? Why does this difference exist, and why does it matter?

This document examines these questions and presents 7 imperatives every IT leader needs to consider when choosing a web filter for their independent school environment.

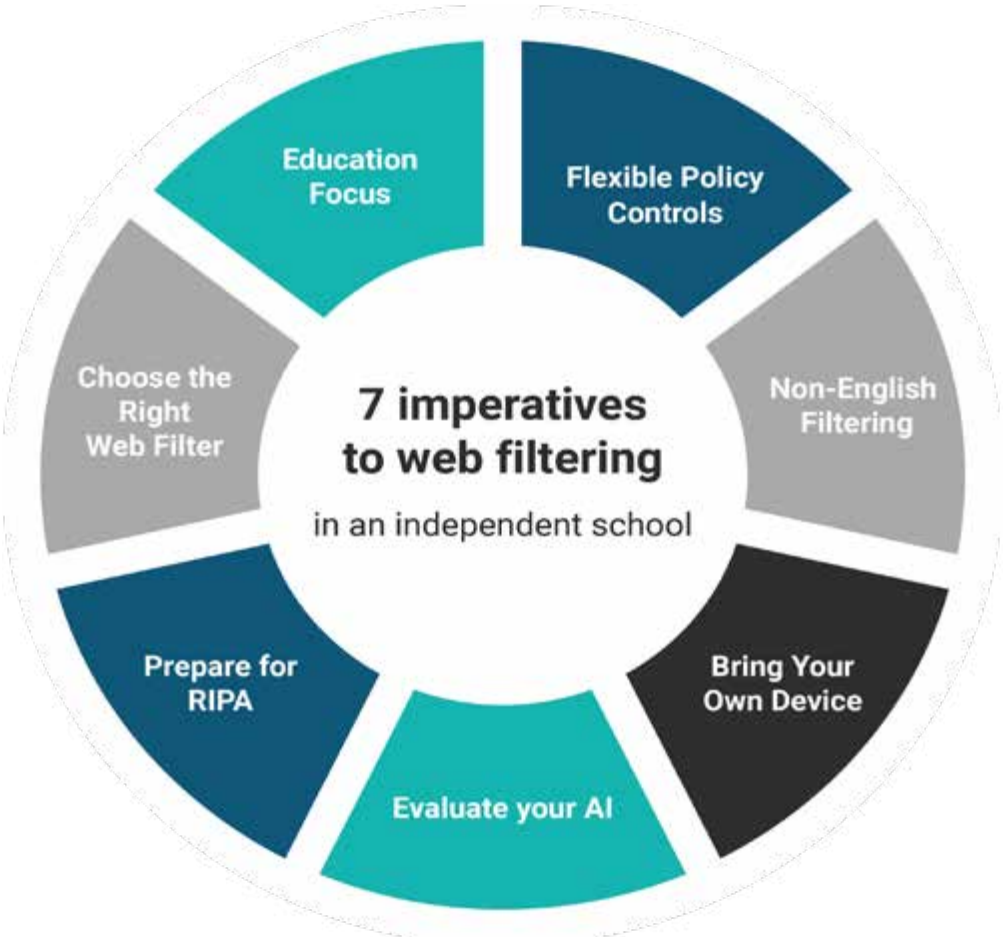
Essential reading for: IT leaders in independent schools in the UK and around the world.

If you have any questions or would like to arrange a demo, please do not hesitate to contact the Smoothwall team.

We'd be happy to help.

Tel: +44 (0)870 1999 500
Email: enquiries@smoothwall.com
Web: www.smoothwall.com/contact

smoothwall®



Imperative 1. Education Focus

The right filter for the right environment

Corporate users have long dominated the direction of IT products and services – and with good reason.

The corporate market is huge, with a projected $3.8 trillion spend in 2019. That's more than the GDP of France. Education meanwhile spends nowhere near as much, and so doesn't get nearly as much attention. This is a challenge, because the needs of education are very different to those of business.

A corporate web filter, for example, might be designed to maximise productivity by denying the major social networks, or to head off a lawsuit by keeping pornography off PCs.

It's likely to serve other functions too, like preventing leaks of sensitive information. A filter is often chosen on the basis of how little impact it will have on day to day operations.

There are a number of education focussed filter vendors. Some offer a strong, premium web filter and safeguarding offering, while others have added these features to a broader set of tools like classroom management.

It's important to set these apart so we know we are doing the best for the young people in our care.

The key signs your web filter wasn't tooled for your educational needs

The filter is an add-on to a security suite

Many security suites from major UTM vendors include URL filtering as an add-on. Often these URL lists have to come from third-party vendors as the company does not maintain their own. These categorise the web's surface and are generally easy to apply as a blanket policy.

They do not include the sort of AI functionality needed to address user-generated content and the websites students often use to work around these types of filter.

Policy tools are limited

It's common to find limited policy tools in standard web filter configurations, with groups pulled from AD and a list of categories to block. Educators know that flexible policies are essential to address the different age and requirements of students, which can vary significantly. Moreover schools are more likely to use diverse systems, or modern cloud-based office suites like GSuite, where a straight AD connection is no longer sufficient.

Diversity of language

Any tool that can't handle unicode domains with non-latin characters, or is unable to scan pages in non-English language will struggle to be effective in a school setting. This is particularly noticeable in filter solutions tacked on to IT management products for schools.

BYOD and authentication

This is another essential requirement, particularly in independent schools. With students wanting to bring their latest iPhone, how can we ensure they're filtered, and that their web usage is logged against their username? DNS based filters are good at blanket filtering, but authenticated access is rarely present.

Logging

Logging is a key component of education safeguarding efforts. Without evidentiary standard logging it's impossible to prove that a user has been doing things they shouldn't. It becomes even more difficult to satisfy a law enforcement request under RIPA.

With additional legislation such as PREVENT being frequently updated, it's important your filter is capable of recording everything.

Education focussed suite

Your filter should be part of an education focussed suite. Some filter vendors produce a web filter and nothing more. Others offer a filter that's part of a larger security suite. This can include tools like DLP and Malware Sandboxing. The sort of tools you might want if you had a security team at your school!

It's advisable for education users to look for filtering technology that comes as part of a wider suite of ed-tech products. Usually these will include digital monitoring tools, perhaps classroom management and record keeping too.

It's also important to consider any integrations offered. Truly education focussed vendors will offer integrations with tools such as MIS, and safeguard record keeping. These kind of integrations are evidence that your vendor cares about your environment and understands the workflows within your school.

Imperative 2. Flexible Policy Controls

Who, what, where and when

Independent schools often have complex needs when it comes to internet access and digital safeguarding.

It's typical to have students that span a broad range of ages, nationalities, and who have a diverse mix of device types. Also students with 24/7 Wi-Fi access from their own devices.

It's a fine balance between giving students the freedom to learn as part of a world class education and the duty of care to protect their wellbeing.

The web filtering policy controls within Smoothwall Filter help independent schools achieve these aims in an intuitive, flexible and powerful policy system.

All Smoothwall Filter policies consist of four elements - Who, What, Where and When.

Who

Typically schools will implement filtering based on age group, with content restricted more heavily for younger pupils. Staff may still have filtering applied, but with a much less restrictive policy. These groups can come from existing authentication systems such as Microsoft Active Directory and Google GSuite. It is also possibly to apply filtering policies to individual users if required.

What

Smoothwall Filter's powerful dynamic content analysis engine powers 200+ categories which gives the ability to apply policies using constantly updated definitions.

Schools can also create their own categories to apply rules, such as walled gardens. These may be used during exams, prep or can be used to limit users to a specific list of websites only.

These rules may also be delegated to staff, who are granted the ability to edit specific portions of the filtering policy.

Where

A school's network is vast and likely covers classrooms, dining areas, sports facilities and boarding houses. The ability to apply differing filtering policies based on the physical location of a user can give powerful controls to the school, such as allowing access to games only from specific places.

When

Not all independent schools will have boarders, but the need to differentiate filtering policies depending on time of day may still be required.

Break times, after-school activities and clubs may require different rules to the main school day. Quota controls can also be used to implement digital wellbeing controls – such as limiting students to 30 minutes social media per day, and only between certain hours and from specific locations.

A premium filter lets you build policies that match the structure and rules of your school. Your school should not have to adapt to meet a filter's rules.

Imperative 3. Non-English Filtering

Independent schools must have a filter capable of handling different languages.

Although English will be the majority of content used for education purposes, it's common for searches for illicit material to start in a student's native language, often because filters pay less attention to this.

For example, 'joc online' is how a Romanian student might search for online games. This gets past the web filter and it's a great way to make new friends! These ad-hoc language lessons are going on in schools around the country.

Domain names are ASCII. ASCII gave a choice of 128 characters, of which the first 30 weren't printable, and capitals and lower-case count as one each. Unsurprisingly, this didn't leave room for accented characters like é, or cyrillic ("russian") characters.

We now have Unicode - a unifying character set that currently offers 137 thousand characters. The most common representation, UTF-8, is used in over 90% of websites, however it is very new to DNS.

What does this mean for web filtering? Even though DNS queries still don't support UTF-8 or Unicode, browsers, (which we update much more often), have taken on the role.

International domains are now translated by the browser. Bücher.de is an example "IDN" - International Domain Name. It's a German bookstore. It's not visible in a DNS lookup – and some web filters fail here too. The browser however will translate it to the ASCII representation xn--bcher-kva.de - which redirects to www.buecher.de

It's important to check two things when considering a premium filter.

1. How well do they categorise search terms in the languages used by your students?

2. Can they filter based on international domain names?

> It's common for searches for illicit material to start in a student's native language, often because filters pay less attention to this.

Imperative 4. Bring Your Own Device

Recreational web filtering

Allowing students to connect their own smartphones, tablets and laptops to the school wireless network is becoming commonplace across secondary and tertiary education. This is particularly relevant to boarding schools who have a need to provide recreational internet access out of school hours.

Students' own devices still need to be authenticated and filtered – so that we know who is using which device and appropriate filtering can be applied.

A combination of two key technologies within Smoothwall Filter make this possible – transparent filtering and 802.1x BYOD authentication.

How this works

Transparent filtering has only a minimal configuration requirement on each device to speak to the filter – all network traffic that passes across the Smoothwall Filter is automatically filtered, and after installation of the HTTPS filtering certificate the secure traffic can be inspected.

802.1x BYOD authentication is an advanced form of network-level authentication. It is possible with Smoothwall Filter to implement authentication like a hotel or conference Wi-Fi – where the user's details are input to a web page when they connect to the wireless.

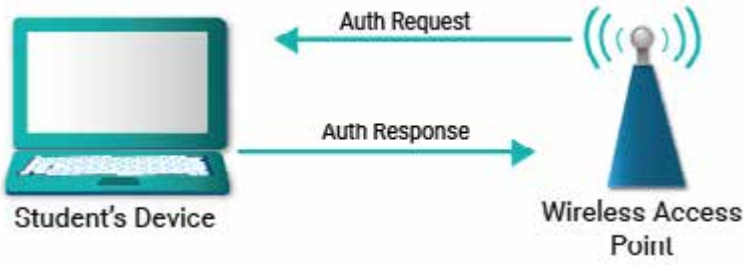
However, having to frequently re-enter credentials can be frustrating for users who connect daily to the network.

802.1x on Smoothwall Filter works in combination with an enterprise wireless network to authenticate the user when they connect (often using WPA2-Enterprise security) and store these credentials on the device.

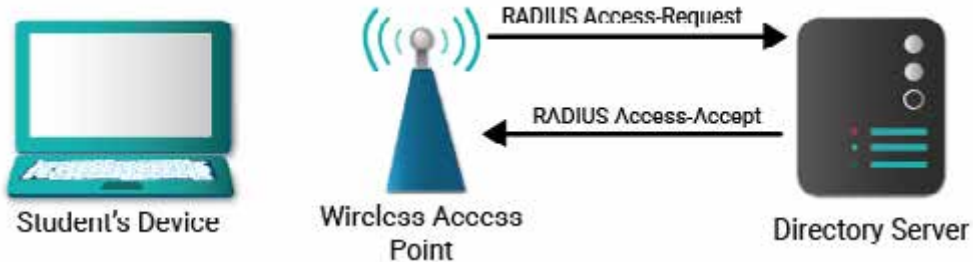
The device will then automatically reconnect to the wireless when in range and provide the credentials without any action needed by the user.

Authentication and filtering on student's own devices

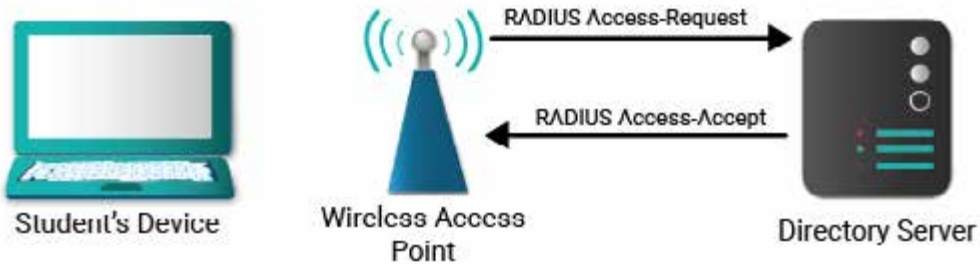
Step 1 - Student connects to the wireless network.



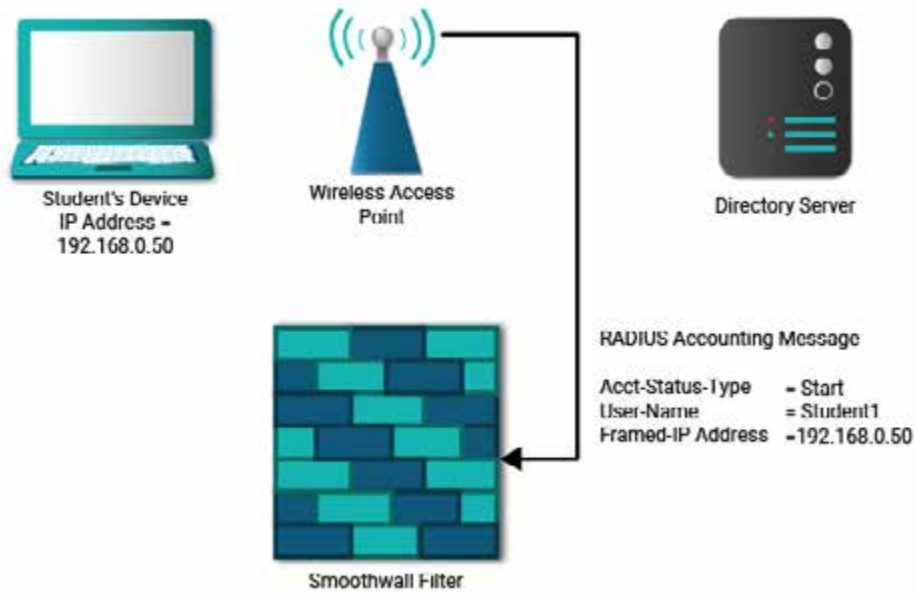
Step 2 - Wireless network sends back authentication request and client provides user-name/password.



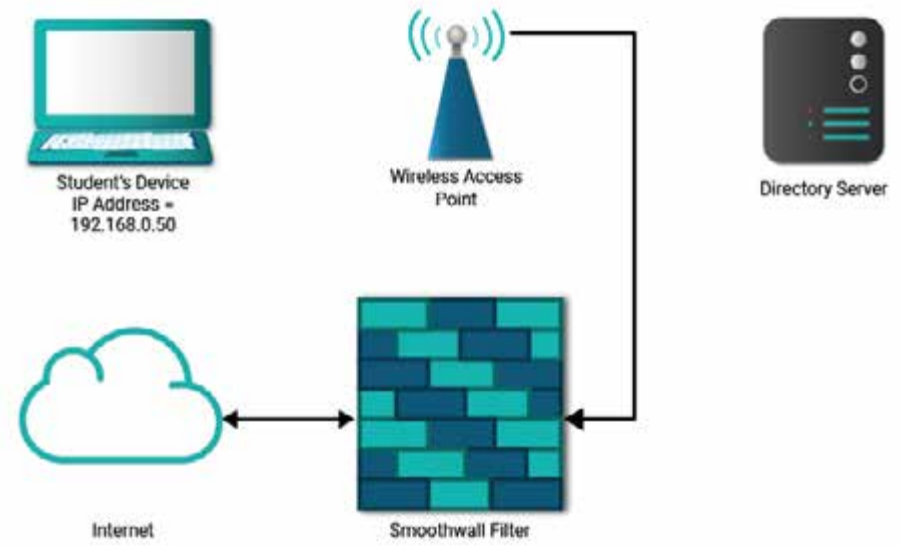
Step 3 - Wireless network validates credentials with a directory service (e.g. Active Directory) using the RADIUS protocol, and receives an acceptance message from the directory server indicating the credentials are correct.



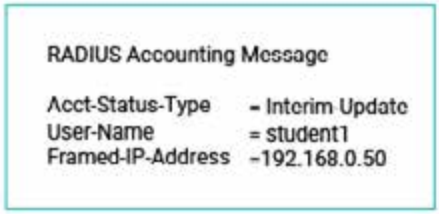
Step 4 - The wireless access point allows the device to connect to the network, an IP address is assigned to the device, and Smoothwall is informed of this new connection.



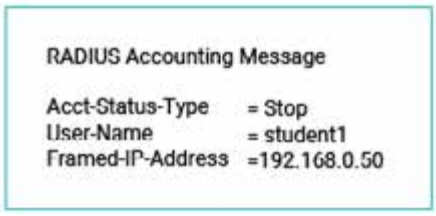
Step 5 - As the user browses the internet, traffic traverses the Smoothwall Filter and the filter knows which filtering policies to apply and with whom to associate the traffic, based on the IP address equalling a specific user-name.



Step 6 - Periodically, the wireless network automatically sends an update to the filter, to let it know that the user is still connected.



Step 7 - When the user disconnects, the wireless network sends a stop message to the filter, so that it knows to no longer associate that IP address with the student.



802.1x BYOD filtering is supported by most enterprise wireless systems which are integrated with directory services. They also need to support RADIUS Accounting with Framed-IP- Addresses. Popular systems include those by Cisco/Meraki, HP/Aruba, Ruckus, Aerohive, and Ubiquiti.

Imperative 5. Evaluate your AI

These days it's unusual to find a web filter vendor not making use of machine learning or intelligence somewhere in their products. But how can you compare them?

Artificial Intelligence systems are essential to keep up with user-generated content and the ever evolving list of filter avoidance tools. These systems are usually effective against similar, but widespread types of content, such as pornographic material, gambling sites or anonymizer tools.

It's difficult to compare the underlying technology however, largely because it's possible to use AI in a multitude of different ways. For example, closed loop learning, human directed learning, and then various models beneath, such as simple HMM or tensorflow. All of these techniques can be applied well or poorly.

The most important question to ask is where does your filter apply these AI techniques?

It's commonly in one of two areas:

1. In line with the web filtering in real-time

Real-time filtering is either baked into a network appliance, or is part of a filtering client. There are occasional updates to the rules database, but generally, the filter makes all decisions locally.

2. Out-of-band offline processing

With out-of-band intelligence, uncategorised URLs are fed back to the filter vendor, and the site is then visited by an automated web crawler or "spider". The results are then passed through the intelligent system, and a categorisation attached to the URL. The categorisation makes it back to the point of filtering in regular URL list updates.

Inlive v out of band comparison

	Inline	Out of band
Speed of reaction	Instant - Any filtering decision is applied straight away, leaving no opportunity for harmful content to get by.	Slow - Unknown content is queued waiting for the offline process to occur. Filtering is then caught up at the next regular update.
Effectiveness: Real-time content	Excellent – Real-time or rapidly changing content is reassessed each time, so a correct decision is made against up to date data.	Poor – Generally the categorisation of a site is either permanently fixed, or fixed for months. This leaves sites with changing content open to misclassification.
Effectiveness: Context	Weak - Inline filters only see one page at a time and can't make decisions based on what's linked to.	Strong – An out-of-band web filter can check a lot of context around the page.
Effectiveness: Logged-in content	Excellent – As these filters work on the data the user sees, even content behind a login such as a forum or social media will get scanned.	Ineffective – The out of band filter sees only the login page, which rarely provides any actionable content.
Additional latency	Low – Usually adding intelligence will add latency to each request. Properly designed systems will limit this so it isn't noticed by the user.	Zero – As all intelligence is out of band, there's no additional latency.

Imperative 6. Prepare for RIPA

In the UK the "Regulation of Investigatory Powers" act (or RIPA) was passed in 2000.

RIPA gives the Police as well as other government bodies such as The Gambling Commission and The Food Standards Agency – a way to access communication data.

For schools, this means that you may be asked to provide information about a user's access to a particular site. This is often in conjunction with PREVENT and tackling extremism but it can be for other purposes too.

Authorities take a dim view of any school unable to provide this kind of information. It's important therefore to consider exactly what your web filter is logging.

- Are all requests authenticated?
- Are all requests logged, including video and image assets – or just the domain?
- Are these logs stored in an appropriate location?
- Are these logs stored in an industry standard format like JSON?
- Are logs kept intact, or is anything discarded to save space?

It's not essential to answer yes to all questions, but it's worth asking potential vendors before you sign up.

Filter logging is important for satisfying law enforcement enquiries, but it's also important for safeguarding incidents, trends and sharing information with DSL colleagues.

A high quality education-focussed filter will offer the level of logging you need. Many standard filters will offer basic reports and little else.

Imperative 7. Choose the Right Filter

No longer an isolated choice

Today's school environment demands that filtering be part of a broader conversation around safeguarding and student protection.

Sometimes a filter will come part of a suite of education focused safeguarding solutions and there can be cost savings by purchasing this way. If not, it's important to consider the other products your filter must work closely with in order to be effective.

Close relatives

The close relatives that can impact on your filter are highlighted below.

Digital Monitoring

Filtering can be closely allied to digital monitoring. Filters can often block these tools from working correctly, or overlap with monitoring, leading to excessive alerting.

Classroom Management

Frequently employed to allow teachers to monitor student behaviour and focus, classroom management tools sometimes include ineffective filtering controls. Better to align your classroom tool with the web filter, and pay once for that feature.

Integrations

Systems that are distinct from the web filter's core role, but should still be considered as potential allies.

Safeguard Record Keeping

The easier it is to get data into your record keeping platform, the better your outcomes will be. The worst option for record keeping is pencil and paper, but a surprising number of schools use this approach.

It's key to ensure your record keeping system can work with your filter and monitor products and can easily accept output from them. For example, attaching a filter log export.

Active Directory

All web filters should integrate with your AD. Ensure you choose a filter that can get user and group level integration from AD.

Google Directory & Google Classroom

GSuite is growing in popularity in UK education, with some schools moving entirely to Google products. Ensure your filter vendor has access to GSuite information. If Google is a strategy for your school, be sure to ask your vendor about their Google expansion plans in the future.

Appendices

Book a demo

Smoothwall is the UK's leading authority on safeguard technology in UK education. Our expertise and pioneering solutions make us the ideal choice for premium schools requiring a premium solution.

Contact us today

To book a free, no obligation demo of any of our solutions or to speak with a technical lead, please contact us. We'd be delighted to help.

Tel: +44 (0)870 1999 500
Email: enquiries@smoothwall.com

smoothwall.com

smoothwall®

Further reading

Web Filtering in Education: Cloud, On-premise or Hybrid?

A complete guide designed to give IT Leaders a thorough insight into the deployment options available to best suit their network needs.

Available at: https://smoothwall.com/web-filtering-deployment

More papers, articles and specs

Visit our website to find more resources dedicated to IT leaders working in the Independent school environment.

Available at: https://smoothwall.com/education/about-you/independents-it-leaders/

About Smoothwall

Smoothwall is the leading digital safeguarding solutions provider in UK Education. 10,000 schools, colleges and academies depend on our filtering and monitoring technologies to keep their students safe and their education organisations compliant.

Since our humble beginnings in 2000 we have been dedicated to empowering educational organisations to digitally safeguard the young people in their care.

Our solutions are innovative and pioneering and developed from the ground up to meet and exceed the legislative requirements set out by the Department for Education, as outlined in the Prevent duty and Keeping Children Safe in Education.

Digital safeguarding solutions were historically seen as security products to be selected, deployed and managed by a school/college's ICT department. And while the ownership remains generally true, the meteoric rise in the use of the internet as a vital tool for learning has firmly placed digital safeguarding on the agenda of most educational stakeholders.

Web filters today are not tools for blocking content.

They are a means of improving learning outcomes by enabling students to freely access rich internet content, protected by granular filtering, controls and alerts to ensure any risks and safeguarding issues are quickly and accurately identified.

Schools/colleges favour Smoothwall because of our understanding of this core concept and our pioneering solutions that support it.

Where Smoothwall Filter dynamically analyses content and intelligently blocks harmful content, Smoothwall Monitor is installed onto the school/college's computers where it analyses on-screen content and any keystrokes made. Words or phrases indicating the user may be at risk of harming or being harmed are captured in a screen shot and sent to the DSL for analysis (or the Smoothwall team if it's a managed service).

Behavioural profiling by monitoring words over time provides an added level of vigilance to enable an early stage help intervention.

As digital learning becomes more commonplace in the classroom, so does safeguarding issues such as mental health, cyberbullying, radicalisation, child sexual exploitation and others.

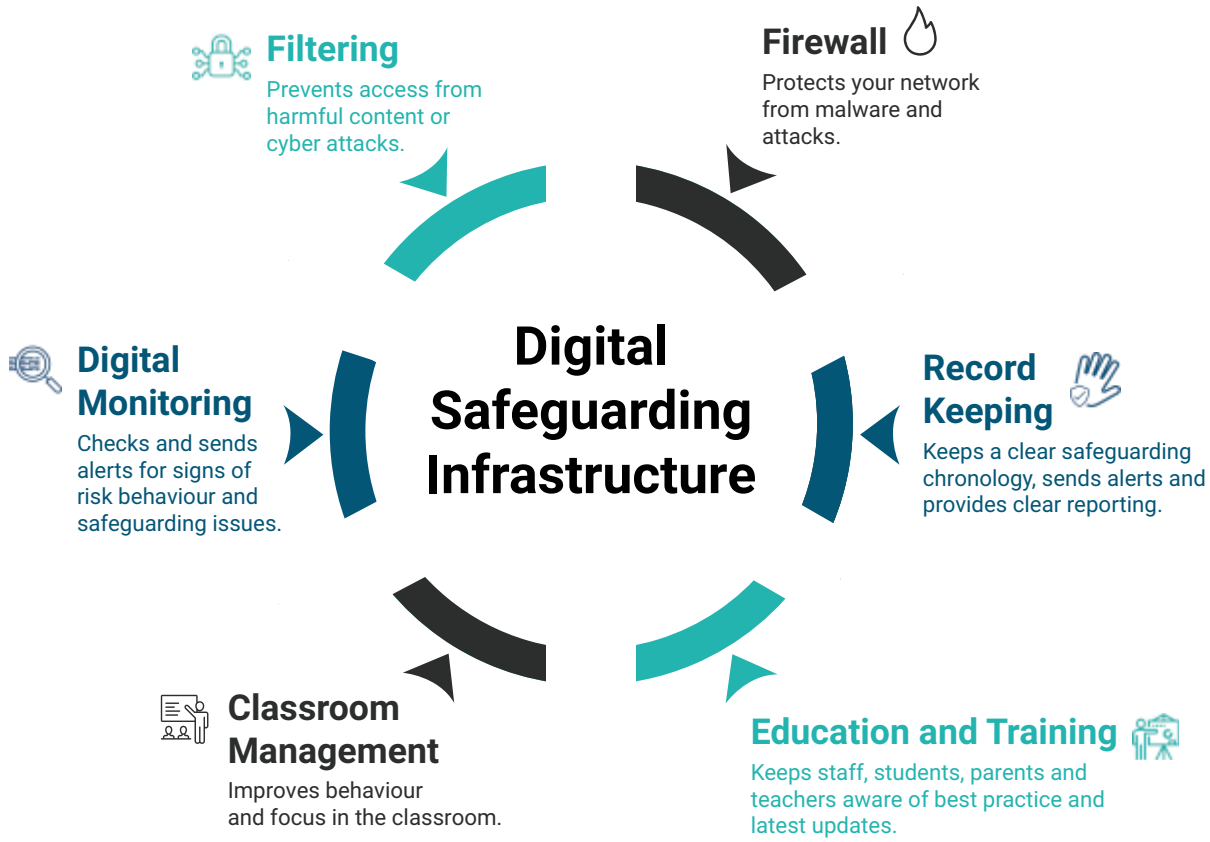
The demands placed on the physical eyes and ears of teachers far exceed their ability to identify all but the most obvious risks, and puts the organisation at odds with both student needs and statutory guidelines.

Smoothwall's robust filtering, firewall, monitoring, classroom management and record keeping provision work in tandem to keep young people safe and your organisation compliant with the legislation, guidelines and recommendations placed upon it.

Continued.

Smoothwall offers a complete online safety infrastructure protecting students at every touch-point.

Our robust filtering, firewall, monitoring, classroom management and record keeping provision work in tandem to keep young people safe and your organisation compliant with the legislation, guidelines and recommendations placed upon it.



Our Partners

IWF

Smoothwall are members of the Internet Watch Foundation (IWF) and implement the Child Abuse Image Content list of domains and URLs.

Home Office

Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

UK Safer Internet Centre

Smoothwall submits details of how our solutions comply with UK legislation. These documents can be accessed on the UK Safer Internet Centre website.

EduGeek

We partner with EduGeek and actively promote the communication platform and information sharing they provide to IT leaders across UK Education.

National Online Safety

Smoothwall exclusively partners with National Online Safety to offer customers their award-winning e-safety training for the whole school community.

Smoothwall

Avalon House
1 Savannah Way
Leeds
West Yorkshire
LS10 1AB

Tel: 44(0) 870 1999 500
Email: enquiries@smoothwall.com

smoothwall.com

Smoothwall
Smoothwall
Smoothwall-ltd
SmoothwallTV

smoothwall®