Smoothwall Insights

A Simple Guide to Web Filtering and Digital Monitoring

The key differences schools, colleges and MATs need to know.

smoothwall.com

smoothwall® by Qoria

Contents

Introduction

As digital technologies play an increasingly central role in students' lives both inside and outside the classroom, web filtering and digital monitoring have become essential components of a setting's safeguarding strategy.

Though often said in the same breath, web filtering and digital monitoring are separate technologies with two specifically different objectives. When implemented correctly, these distinct processes work in tandem to mitigate digital risks and help organisations to achieve high levels of protection for their students.

This guide provides DSLs, IT teams, SLTs and governors, with clear definitions of these fundamental pillars of digital safeguarding.

Essential reading for: Headteachers, IT Managers, DSLs, Governors, Proprietors, and anyone interested in or responsible for safeguarding compliance within a school, college or MAT.

1.0 What is Web Filtering?

Web filters manage access to internet pages or websites, with the aim of mitigating opportunities for individuals to reach harmful or inappropriate content.

A helpful way to understand the role of web filters is to view them as a playground fence. They prevent potentially dangerous influences from entering the school, and stop children from wandering into unsafe scenarios. Importantly, web filters are not impenetrable walls - they still facilitate the movement of traffic in and out to ensure the school can function effectively.

1.1 Not just a tool that blocks

A common misconception about web filtering is that it is largely about blocking content in order to limit what students can access on the internet.

On the surface this is true, but the somewhat negative perception of web filtering as a tool of restriction fails to recognise the potential freedom it can provide for students and teachers. A more accurate way to view web filtering is as a tool that allows rather than blocks. By thoughtfully reducing access to harmful content, organisations can provide students with the opportunity to safely explore the internet in a way that promotes productive learning and allows them to develop into responsible digital citizens.

Striking the right balance

Underblocking

When a web filter fails to limit access to inappropriate web pages, leaving students exposed to potentially harmful content.

Overblocking

When a web filter restricts access to non-harmful web pages that could be useful in a teaching and learning environment.

The Department for Education advises that "filtering system[s] should block harmful and inappropriate content, without unreasonably impacting teaching and learning."

While underblocking web pages can leave students exposed to inappropriate content, overblocking may cause just as much harm. As early as 2010, Ofsted observed that "pupils were more vulnerable overall when schools used locked-down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves." (Ofsted, **The Safe Use of New Technologies).**

It's important for students to be able to safely explore the internet, because it helps them to develop key abilities including critical thinking and research and problem solving skills.

> A more accurate way to view web filtering is as a tool that **allows** rather than blocks."

1.2 Types of web filter used in UK education

DNS filters

These web filters rely on a pre-selected list of banned domain names to restrict content. If a person attempts to visit a page on a website that appears on the list of banned domains, it will be blocked by the filter. This rudimentary approach results in both overblocking and underblocking, and potential exposure to risk remains high.

URL filters

URL web filters block specific web pages instead of entire websites. For example, certain pages of Wikipedia may be accessible, but those covering potentially inappropriate topics can be restricted. URL filters still rely on static blocklists, meaning they cannot assess new or changing content and may still cause overblocking and underblocking.

Content-aware filters

Content-aware web filters assess the actual content of a web page to judge whether to restrict it or not. This sophisticated approach allows more flexibility and freedom than DNS or URL filtering. However, such filters may rely on historical assessments of web pages, which means risk of exposure to harmful content remains - particularly when it comes to new or updated content.

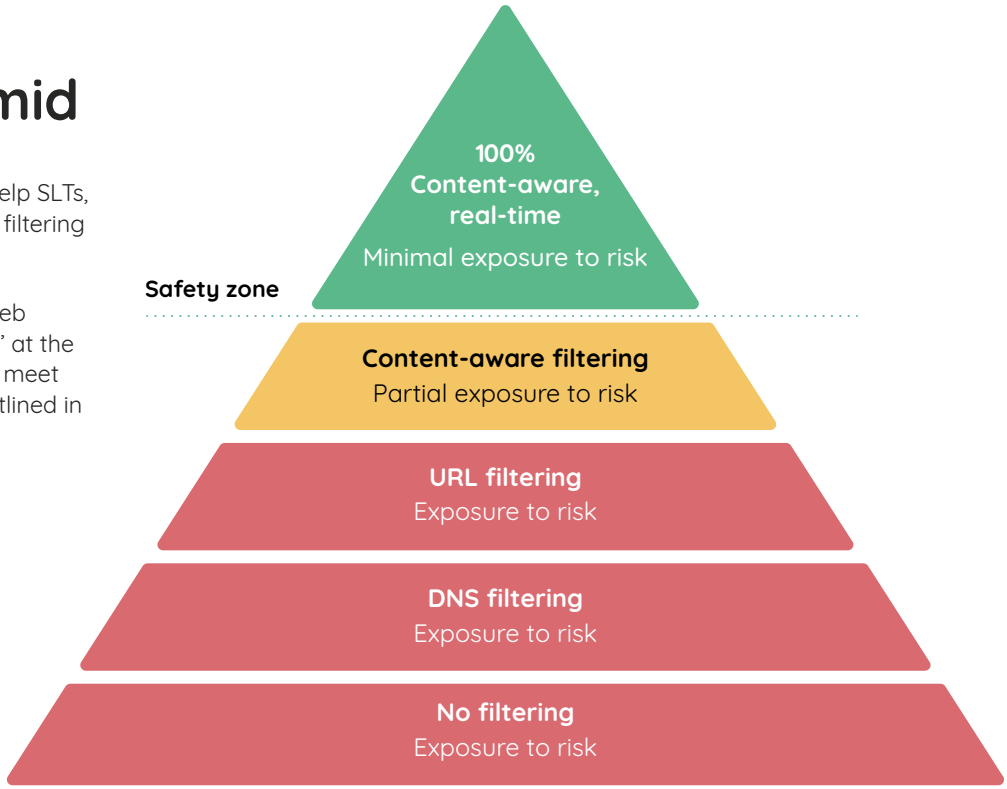
Real-time, content-aware filters

These dynamic web filters assess the content, context and construction of web pages in real-time. The filter reacts as users explore the internet, leaving little to no delay between harmful content being uploaded and access to it being restricted. Students can enjoy a rich learning experience, as content deemed to be educational remains accessible, even when similar pages on the same website are blocked.

The Filter Safety Pyramid

Our Filter Safety Pyramid can help SLTs, DSLs and IT staff identify which filtering solutions are fit for purpose.

For educational settings, only web filters that sit in the 'safety zone' at the top of the Filter Safety Pyramid meet 'appropriate' levels of safety outlined in statutory guidance.



2.0 What is Digital Monitoring?

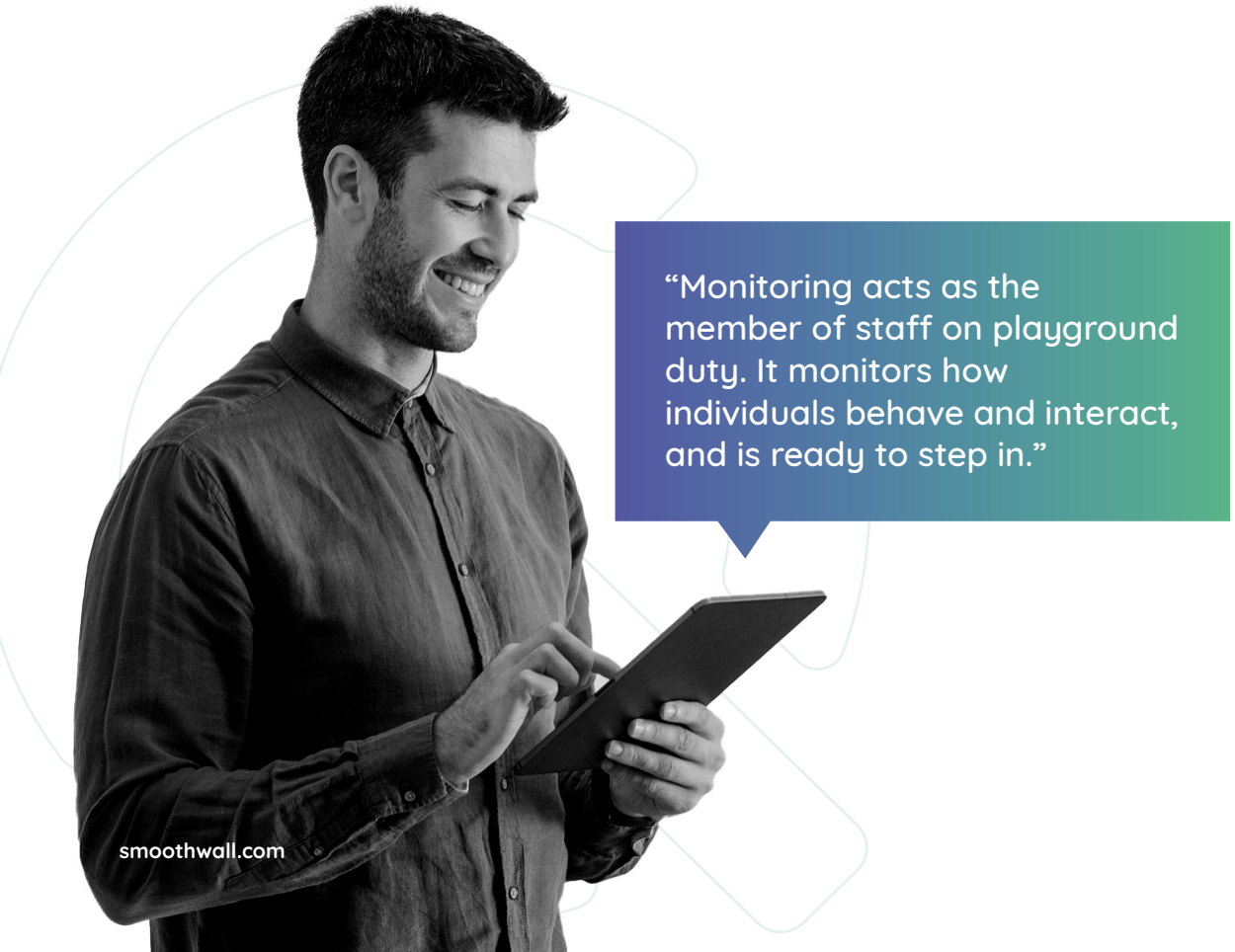
Digital monitoring refers to the process by which activity on devices (desktop, laptops, tablets and phones) is monitored **to identify potential risks or breaches of policy.**

To continue the schoolyard analogy, monitoring acts as the member of staff on playground duty. It watches how individuals behave and interact, and is ready to step in should it become apparent that an individual requires help, or a potentially harmful incident is developing.

2.1 How does digital monitoring work?

To implement digital monitoring, a monitoring client, or "agent", is installed on school-managed devices. This software sits in the background monitoring the digital activity of device users. If words or behaviours deemed to be potentially harmful are identified, an alert is generated and sent to the relevant administrator (often the DSL and/or IT Manager).

Not all monitoring requires a software-based solution. In settings with low risk profiles, where direct supervision of device use is achievable, physical monitoring may be adequate. However, such conditions are unlikely to be attainable for a majority of schools, colleges and MATs.



2.2 Types of digital monitoring

There are 2 main approaches to digital monitoring:
managed and unmanaged.

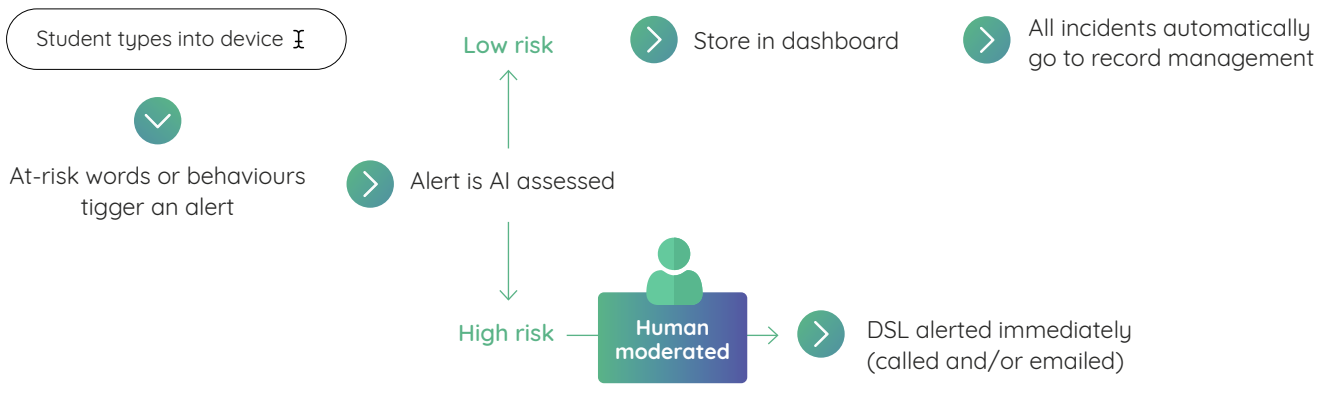
Unmanaged	Managed (or moderated)
Agent stored on the device	Agent stored on the device
Entirely keyword based	Alerts checked by humans & AI
Electronic alters only	Phone calls for serious events
No context provided	Context and depth available
More likely to have a high rate of false positives	Very low false positives because an informed judgement is made

Unmanaged monitoring systems

Unmanaged digital monitoring systems are keyword-based, meaning an alert is triggered when a user types a specific word, for example, “bomb” into a device. The problem with this approach is that it does not take context into account, which in many cases can reveal the difference between a potential risk and an innocent action. For example, a student could type, “How to build a bomb”, or “Who invented the atom bomb?”. In both cases an unmanaged system is likely to send an alert to administrators.

Managed monitoring systems

Managed digital monitoring systems utilise AI technology and human moderation to categorise alerts into different levels of risk and reduce false positives. Incidents are considered within the context that they happened, and when risks are judged to be legitimate, the context can be shared with administrators in the form of screenshots. You can see an example of how a managed digital monitoring system works in the diagram below.



3.0 Web Filtering vs Digital Monitoring: Key differences

Web Filtering	Digital Monitoring
Web filtering is reactive	Digital monitoring is proactive
Web filtering applies to online content	Digital monitoring can apply to online and offline content
Web filtering manages access	Digital monitoring manages behaviours
Web filtering is managed by IT teams	Digital monitoring is managed by DSL teams

4.0 Why do Educational Settings Need Both?

The risks posed by the current digital landscape require a two-pronged approach to ensure that threats can be identified and removed in a timely manner.

A clear understanding of the difference between web filtering and digital monitoring reveals how essential it is for schools, colleges and MATs to implement both of these provisions. The two solutions complement one another - merging to form a robust digital safeguarding framework.

> They sound similar, but they're quite different, and they've both got such important roles that **they're both needed in a school to safeguard your children."**
>
> Ruth Noble,
> DSL Tonacliffe Primary School

4.1 The individual limitations of web filtering and digital monitoring

Why web filtering needs digital monitoring

Web filters are responsive tools that manage access to online content. They cannot:

- Assess content being created by network users
- Restrict inappropriate offline content
- Provide in-depth context for user behaviours

Educational organisations also have to contend with the fact that the students they are tasked with protecting can be incredibly tech-savvy and utilise both online and offline platforms for a range of different uses. This means that websites or programmes considered "safe" can still host harmful behaviours.

For example, students can use word processing documents to write manifestos, or take advantage of chat functions on otherwise harmless platforms to send abusive messages to others.

Such incidents are unlikely to be prevented or identified by physical monitoring or web filtering.

In 2023

Data from **Smoothwall Monitor** reveals the extent to which potential digital safeguarding risks occur even with advanced web filtering in place:

Every 2 minutes

Smoothwall Monitor detected a student suspected to be at **serious risk**

Every 7 minutes

Smoothwall Monitor found a child suspected to be involved in a **serious sexual incident**

Every 11 minutes

Smoothwall Monitor found a suspected **vulnerable child**

Why digital monitoring needs web filtering

Digital monitoring solutions are designed to empower DSLs to work more efficiently and effectively. They act as an extra pair of eyes and ears, detecting hidden risks that a DSL is unlikely to see.

By reducing the need for manual tasks, such as sifting through reports, and allowing them to identify potential risks early, this technology enables DSLs to use their expertise to resolve incidents swiftly and prevent issues from escalating into serious problems.

However, without effective web filtering in place, these systems run the risk of being overloaded with incidents, which undermines their ability to reduce workloads for safeguarding teams.

4.2 Working in tandem to tackle today's threats

According to **2024 research from Internet Matters,** over 2/3 of UK children report experiencing online harms. Two of the most common risks schools have to deal with are exposure to harmful content and cyberbullying.

Exposure to harmful content

A March 2024 **research report from Family Kids & Youth**, commissioned by Ofcom, reveals the unsettling reality of children's exposure to violent content:

- Children described encountering violent content as "unavoidable"
- Children reported first seeing violent online content in primary school
- Children were encountering violent content without seeking it out

The fast-moving nature of online content poses a significant challenge to safeguarders trying to protect children from digital harms.

According to the report:

"Teachers felt the rate of technological change within platforms means that by the time they have become aware of the content, it is no longer viral and has been replaced with new violent content."

Utilising a real-time, content-aware web filter can help organisations overcome this disadvantage by blocking violent content as soon as it goes live. Any inappropriate content that manages to evade the web filter should be identified by a setting's digital monitoring system.

This can quickly alert DSLs to the issue, prevent users from sharing the content and provide context as to where the material was accessed.

> By the time they have become aware of the content, it is no longer viral and has been **replaced with new violent content."**
>
> Understanding Pathways to Online Violent Content Among Children, Family Kids & Youth

The Impact of Digital Monitoring on Cyberbullying

Digital platforms offer a level of anonymity and access to other people that can facilitate cyberbullying. **A 2024 study from the National Centre for Social Research** found that: "Children, school staff and practitioners reported that cyberbullying happened anywhere children interacted online."

Such incidents are incredibly hard for DSLs to spot, as they occur in a wide range of settings and evidence can be deleted at the touch of a button. Not only can digital monitoring increase visibility of cyberbullying, but the knowledge that devices are being monitored can be a deterrent to these behaviours in itself.

In addition, if it becomes apparent that specific apps or web pages are being used to conduct cyberbullying, web filters can be adjusted to restrict access to them.

In 2023, every **6 minutes** Smoothwall Monitor found a child suspected to be involved in a **serious cyberbullying, bullying or violent incident.**

4.3 Meeting statutory guidelines

According to the Department for Education, filtering and monitoring **are mandatory components** of a digital safeguarding strategy.

The filtering and monitoring standards for schools and colleges is the blueprint that outlines the criteria schools, colleges and MATs should already be meeting.

The 4 standards are:

- Identify and assign roles and responsibilities
- Review filtering and monitoring systems at least annually
- Filters should block harmful and inappropriate content, without unreasonably impacting teaching and learning
- Monitoring strategies should meet the safeguarding needs of your setting

SLTs, IT teams and DSLs should **read the guidelines** in full, as they provide key details on the requirements needed to meet the standards.

Keeping Children Safe in Education (KCSIE)

KCSIE emphasises how crucial it is for organisations to protect their students from online harms, and states that "as part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place."

Echoing guidance from the DfE's filtering and monitoring standards, KCSIE highlights the need to review the effectiveness of filtering and monitoring systems "at least annually."

Regular assessments help schools and colleges to ensure that web filtering and digital monitoring solutions are up to date and working correctly, so that students are receiving the highest possible level of protection.

The document also emphasises the need for educational organisations to provide regular online safety training, to ensure that staff continue to have the "relevant skills and knowledge to safeguard children effectively." DSLs are required to have a clear understanding of the web filtering and digital monitoring systems in their setting, but every member of staff should know how to identify and report digital safeguarding concerns.

UK SIC definitions

While there are clear standards dictating what schools, colleges and MATs need to achieve with web filtering and digital monitoring, how each organisation fulfils its obligations in this area will look different. Organisations should perform risk assessments to establish the type of solutions they require to keep students safe.

Two valuable resources that schools and colleges can consult during this process are the **appropriate filtering** and **appropriate monitoring** guidelines from the UK Safer Internet Centre (UK SIC).

> "The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges."
>
> KCSIE, 2024

Approved by the Department for Education, these guidelines cover:

- Features to look for in monitoring/filtering providers or systems
- The types of inappropriate content filters should block
- The types of content monitoring systems should manage
- Principles that filtering and monitoring systems should meet

SLTs, governors, DSLs and IT staff should work together to ensure that their setting utilises effective web filtering and digital monitoring.

5.0 Solutions by Smoothwall

To further understand the distinctions between web filtering and digital monitoring, let's explore the specifications of two solutions designed from the ground up for use in education settings.

These stand alone solutions can work together to form the foundation of a powerful digital safeguarding strategy.

5.1 Smoothwall Filter

Smoothwall Filter is the only 100% real-time, content-aware web filter on the market. Trusted by 1 in 3 schools, its key features include:

Dynamic content analysis

It assesses the content, context and construction of every web page in real time, ensuring that harmful content is blocked as soon as it goes live.

Granular control

Filtering can be tailored for specific user groups, content categories, times and location IPs to allow students to enjoy safe, age and time-appropriate online experiences.

Notifications and reports

It notifies of incidents across 7 category rule sets and enables reporting on search behaviours by individuals or groups, to support investigations.

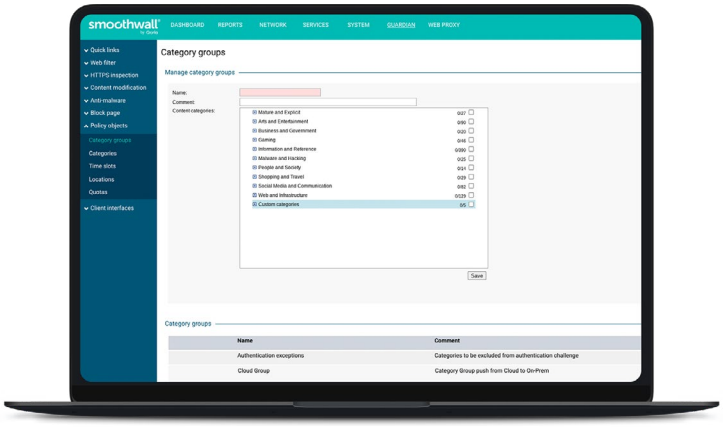
Works behind HTTPS

It detects harmful or malicious content that is hidden, for example behind Secure Socket Layer (SSL) and secure anonymous proxies.

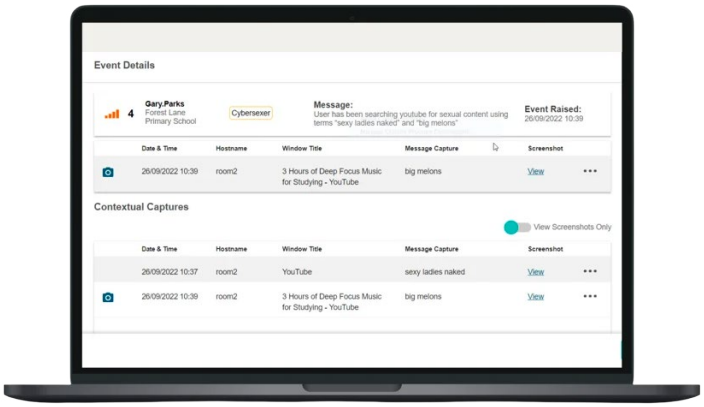
IT leaders have a choice of on-premise, cloud or hybrid deployment, to ensure that Smoothwall Filter adapts to the setting's specific needs.

"It's hard to find a system that you can train staff on. Everything's in its place, everything's super easy to navigate."

Thomas Kates, IT & Commercial Manager, Boundary Oak School and Conifers School, QV Education



5.2 Smoothwall Monitor



Smoothwall Monitor is a real-time, human-moderated digital monitoring system. It alerts DSLs to incidents such as cyberbullying, sharing of sexual content and inappropriate online conversations, so that they can practise early intervention to reduce serious events.

Key features include:

Real-time alerts

DSLs receive alerts within minutes of an event being detected. Notifications are sent by email or phone, depending on the level of suspected risk. Lower level alerts are stored in a database for staff to review at their convenience.

24/7 Human moderation

An experienced team of human moderators provide round the clock protection, 365 days a year. They assess all serious alerts to reduce false positives and ensure that DSLs are only contacted when necessary.

Works online and offline

Suspected risks are detected even when devices are disconnected from the internet - when the device reconnects, data is transmitted for analysis.

Deployment of Smoothwall Monitor is entirely cloud-based, so there is no burden on IT teams.

> The biggest thing that we've found is that it covers all of those requirements that you have to have. From the outside looking in you are covering all of your bases, and from the inside looking out you know you're doing the best for your kids and protecting them as best you can."
>
> Ann Rose, Computing & E-Safety Lead at Hollywood Primary School

6.0 A Cohesive Digital Safeguarding Strategy for Schools, Colleges and MATs

Web filters and digital monitoring solutions are a complementary set of technologies - you can't afford to have one without the other.

Together, they form a solid foundation for a digital safeguarding strategy, helping schools, colleges and MATs to keep pupils safe while offering them the freedom to learn without limits.

When implemented correctly, these provisions:

- Shield students from digital threats that occur both online and offline
- Strengthen a setting's cybersecurity by protecting networks
- Reduce workloads and improve efficiency for DSLs & IT teams
- Enable organisations to meet, and even exceed, their statutory obligations

The digital age poses a range of challenges to schools, colleges and MATs, and effective digital safeguarding requires something of a balancing act. Web filtering and digital monitoring work hand-in-hand to establish a safe learning environment in which students can be nurtured into confident, responsible device users.

Let's talk

To learn how to implement effective web filtering and/or digital monitoring in your school, college or MAT, or request a free demo of our solutions, get in touch today.

Contact: enquiries@smoothwall.com
Visit: www.smoothwall.com

We're ready 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