Smoothwall Insights

Bridging the Language Gap

A guide to digital safeguarding technology for non-technical DSLs.

smoothwall.com

smoothwall® by Qoria

Contents

About this Document

DSLs regularly tell us that they want a better understanding of the digital safeguarding technologies their school is using.

They want to reassure themselves that best practice is being followed and that they are up to speed with the wider technologies available to keep their children safe and their school compliant.

The difficulty arises in the language gap that often exists between technical and non-technical colleagues.

DSLs don't always know the right questions to ask and when they do, they may not fully understand the answer.

Conversely IT teams don't always know what information a DSL might need.

A language barrier like this can be damaging to a school's safeguarding strategy. It can negatively impact an Ofsted inspection and cause stress and anxiety on the part of the DSL who may already be juggling multiple responsibilities.

This guide has been written to bridge that gap. It is a practical and helpful resource to help demystify the technicalities of digital safeguarding solutions.

Essential reading for: Headteachers, DSL, Governors and anyone with a non-technical responsibility for ensuring digital safety within schools or colleges.

Foreword - The Key

Today's children are growing up in a digital world. This interconnected world offers many opportunities for learning but also poses risks to safety and well-being.

Just over 1 in 5 girls aged 11 to 18 said they had received a request for a sexual image or message, according to a recent NSPCC survey. There's been a year-on-year increase in the number and rate of online child sexual offences. The same survey also found that a quarter of primary school children and a third of secondary school pupils report seeing bullying online.

On top of the risks, it's a fast changing area, which can make it even harder to keep children safe online.

Filtering and monitoring systems are one piece of the puzzle, and the DfE expects you to have appropriate systems in place. These tools help you safeguard your pupils by restricting and monitoring what children are viewing in school. They'll stop children accessing inappropriate sites and content, and alert you to potential issues.

Having peace of mind that good filtering and monitoring technology is in place will allow you to focus on other aspects of safeguarding pupils.

This guide aims to help you understand how these tools work and help you choose the right systems for your school.

Our members have told us that online safety is one of their biggest safeguarding training priorities over this school year, and under Keeping Children Safe in Education, you're expected to cover online safety in your safeguarding training.

That's why we included a section in our INSET pack and a chapter in our Safeguarding Essentials elearning course dedicated to online safety, and will continue to produce resources to help you keep children safe online.
Chris Kenyon, CEO at The Key

The Key

Section 1. Web Filtering

1.1 What is web filtering?

Web filtering systems sit on your school server or in the cloud and prevent students from accessing content on the internet that may be harmful or inappropriate. Keeping Children Safe in Education (KCSIE) and Ofsted expect filtering as an essential safeguarding function. It is not possible to successfully safeguard your school without good web filtering. There are generally two types of filtering.

DNS filtering

- DNS filtering is the most basic kind of filtering.
- It matches what a person types into a web browser with a master list (blocklist) of banned URLs.
- If there's a match, the site is blocked and the pupil can't view the site.
- DNS filtering is a cheaper option and usually comes bundled with other services, such as broadband.
- The downside to this is it can take anything up to 6 months before DNS filters sync with the blocklist and update themselves.
- With new content going live on the internet every second, that's a substantial amount of time your students are exposed to potentially harmful content. Even if the sync happened within 24 hours, that's still too long.

Real-time content aware filtering

- Real-time content filtering checks every web page for suitability immediately before it appears on screen.
- Appropriate content appears, whereas anything that may be harmful is blocked.
- There is no delay between new potentially harmful content going live on the internet and it being blocked from students.
- This type of filtering is also 'granular'. This means that each page is checked for its content, context and construction before being blocked or allowed.
- For example, the word 'killer' in the copy might suggest inappropriate content. But a second check at the context may reveal a site talking about a 'blog containing excellent, killer information on a topic'.
- This three-stage check minimises false positives and ensures that pupils are protected, without overblocking and therefore negatively impacting on learning.

Web filtering - the impact on lessons and learning

Web filtering is not just about protecting students from harmful content.

Effective filtering can enhance lessons by allowing students the freedom to use the internet to learn in a fun and more productive way and still be safe.

A basic filter is likely to overblock and so restrict what content students can see and what teachers are able to use to support their teaching.

Statutory guidelines advise schools to check that their system is not so locked down that overblocking occurs. The speed of filtering can also impact on lessons. For example, some systems will slow down or block due to media use or file sharing.

When using graphic design packages in an art lesson or using video for a media project, the type of filtering system can impact on the usability of your devices. Some filtering systems are able to provide bandwidth management so that you can control what is used and where.

1.2 Key terms unpicked

There is lots of terminology used around web filtering. The key terms appear below.

Real-time dynamic content analysis
This function means that the filtering system will look at the content on a web page in real-time. It will analyse the words and images, together with the context and construction of the page.

Any content that may appear inappropriate is then blocked. For example, the word 'killer' but whose context reveals otherwise, for example, 'excellent, killer ideas' is allowed through. This reduces false positives and prevents overblocking.

Whitelist
This is a list of trusted domains that will always be allowed through your filter.

Having a whitelist can conserve system resources and ensure important sites are not unintentionally blocked.

Categories
Filtering categorises sites into themes to establish what access is and isn't allowed.

For example, a category might include banned content types such as radicalisation or violence, or might include allowed content types such as game sites, education and reference, or medical information sites.

HTTPS filtering
HTTPS refers to an encrypted secure connection. You may be familiar with these on e-commerce websites or other password protected pages.

Nowadays, the whole web is moving over to HTTPS to legitimise websites and draw attention to those that are not. A website which is on HTTPS will have a small picture of a lock in the IP address bar.

BYOD (bring your own device)
Own devices brought into school by staff and students are more likely to put your school's systems under threat as they have not been managed and set-up by your own IT teams. You should ensure they are sufficiently filtered too. Look out for web filtering products that cover BYOD.

Students circumventing filter and proxy blocking

It is not uncommon for some students to try and circumvent your school's filter. Capable students may be technically savvy enough to direct their browsing through an unknown proxy server so that their web surfing goes under your radar.

Smoothwall's engineers are well aware of the tactics students use and are many steps ahead. Proxy-blocking is the function they use to stop them.

Check that your filtering provider includes proxy-blocking in order to block any traffic that comes through unknown proxies.

Granularity (multi age-group/user requirements)

It's likely that you will want different settings for different user groups within your school. This is called granular filtering and it gives flexibility for ensuring age-appropriate learning.

It enables you to provide a wide variety of resources for older students that may be inappropriate for younger students. For example, students studying A-Level Music may need access to clips from the film Psycho as it is part of the syllabus. It is an age 15 certificate and therefore not appropriate for younger students.

Granular filtering is also useful for specific time periods too, such as students attending out of school clubs or breakfast clubs, or older students taking part in out of hours study groups. Or even teachers attending school on inset days when no children are present.

Anti-malware and anti-ransomware

Malware is a blanket term used to describe types of malicious software, viruses and code that could damage your systems. Malware is hard to control within a school and can be likened to trying to avoid tummy bugs and colds coming into your community.

You'll likely have a whole network of different devices and operating systems with files coming in from on and off-site.

If a student sends an infected assignment to a teacher, or someone clicks on an infected ad on a website, it's important to ensure your school systems are sufficiently secured.

Anti-malware is a type of software that scans for these types of bugs and viruses to make sure that none can slip through into your system.

Layer 7 application control

Layer 7 application control is a tool your Network Managers use to identify and stop unwanted applications on your network so that you can prioritise the applications you do want.

This can be handy especially when filtering unmanaged (non-school) devices on the network. And can be particularly useful when students are using personal devices.

Social media controls

It can be tricky deciding how much social media freedom to give students in school. Some schools block all social media. However, with this generation growing up in a connected world in which social media plays a key part, some access to social media can aid learning and also allow students to communicate.

For instance, politicians and social activist groups will often communicate through social media, and teachers may want to use this as a lesson resource.

When allowing social media access, you should ensure that your filter allows for varied access control. For example, read-only access. Also the ability to choose which social media apps are available, as well as different settings for different ages and so on.

Bandwidth management

Basic filters can sometimes cause bandwidth problems. This can be particularly problematic when large media files or file sharing takes places - usually in multi-media or design classes. This can impact on or even halt the school network and negatively affecting lesson time.

Bandwidth management allows you to control where your bandwidth is being used in real-time. For instance, if you have a department using a large amount of bandwidth for media file usage you can distribute the bandwidth differently so that it doesn’t impact on systems.

Deployment

Deployment is the means by which your school hosts your filter and other applications. You may come across different terms relating to deployment. For example, cloud, on-premise or hybrid deployment.

Your IT leaders will likely have considered which deployment is right for your school. An explanation of each one appears below. A good filter provider, such as Smoothwall, will accommodate all options.

On-premise
An on-premise solution means your filtering is hosted on a server within your school. This is the traditional option and good for schools that have the technical team on-site to manage the system.

Your school may have invested in expensive servers in the past and may want to wait until cloud filtering has matured before making the move over to cloud-based filtering.

Cloud
This means that your filtering works in the cloud and has no need for expensive hardware on-site. This option is often called elastic because it is so easily scalable if your number of devices changes year by year.

A cloud solution can also free up your IT staff to focus on all the other rising demands of IT work needed in school.

Hybrid
Hybrid means that your solution uses both cloud and on-premise. This can be a good solution when you have already invested in expensive servers and have a network of computers that are working effectively on filtering but need to add to the network in some way. For example, using portable devices that might work more effectively in cloud filtering.

1.3 Knowing the best filter fit for your school/college

When purchasing your filter, your IT colleagues will likely have considered a number of factors. The table below explains what these are so you can better understand the decision they made.

	Benefits	Drawbacks	Best fit
Cloud filtering	Easy to scale. No hardware on site so no expensive outlay. Can change subscription overtime.	May be difficult to customise if your IT set-up is complicated.	Schools that have straight forward set-ups. Schools that don't want to invest in expensive IT infrastructure costs. Schools in which IT set-ups need to be flexible to allow for increase/decrease in devices. Schools that need IT staff time to be freed up.
On-premise filtering	Good for schools with BYOD.	Can be difficult and expensive to add more devices onto your network. Can have issues with bottlenecks from chokepoints.	Schools that want to stick with a set-up that works for them. Schools that have already purchased expensive hardware. Schools that want to keep filtering as capital expenditure from other funds rather than the everyday IT budget.
Hybrid filtering	Gives maximum flexibility. Can help with load distribution.	Will need tech to understand both on-premise and cloud set-ups.	Can be useful for adding off-site or BYOD filtering to a school with on-premise set-up.

	Benefits	Drawbacks	Best fit
Layer 7 application control	Allows you to control which applications run and have priority.	May need technical expertise.	Schools that want good control over the applications running on their network.
Bandwidth management	Schools can allocate bandwidth so that high media usage and file sharing can be managed.	Will require technical management.	Best for schools in which some lessons take a high volume of bandwidth and requires allocation for distribution.
Granularity	You can change settings intricately depending on user types / ages.	May take some technical input.	Schools covering different key stages that require different settings for different ages/user groups.
Customisation	Flexibility in your individual requirements to map filtering specifically to your school.	Can take longer to set-up.	Schools that have complicated set-ups with different types of devices on the network.
Blocking anonymous proxies	Students can be stopped from using anonymous proxies, keeping your network protected.	None.	Schools which have students managing to circumvent their filters through anonymous proxies.

1.4 Reviewing your filtering

This section is designed to help you understand the level of filtering protection your school has.

Use the questions below to discuss your current provision with IT. Use the tick boxes at the side to highlight any points you want to follow-up on later.

Have there been any network problems in our filtering due to bottlenecks from chokepoints? Were we able to resolve the issue?

□ **Yes** — If there have been issues with this, it may mean that you need to look at changing your system over to a cloud-based option.

□ **No** — This is not an issue you need to consider when reviewing your filtering.

□ **Unsure** — You may need to check with your vendor.

Is our school filtering set-up to provide different filtering for different user groups?

□ **Yes** — You have a flexible filtering solution. Check that you are happy with the settings for the different user groups.

□ **No** — Consider whether this is putting any restriction on class teaching.
Ask teaching staff if they have enough access to resources for different age ranges.
Consider whether this needs to be introduced and find out if your current filtering system has that option or not.

Does our filtering system use real-time content analysis?

□ **Yes** — You can be sure that even recent out of date content is filtered appropriately.

□ **No** — You may want to review this and find a solution not based on blocklists.

□ **Unsure** — Check with your vendor.

Does our filtering system allow for bandwidth management?

□ **Yes** — Your IT team can manage bandwidth and therefore minimise the impact of large media files or file-sharing.

□ **No** — IT colleagues may say that they have been experiencing a slow network and even crashing because of constraints on bandwidth.

□ **Unsure** — Check with your vendor.

Does our filtering provider protect data privacy?

□ **Yes**
Yes, the school's providers have supplied privacy statements or security certificates to assure you that all data is kept at maximum security.

□ **No**
You should consider what sensitive data could be at risk and consider whether you should change to a more secure provider.

□ **Unsure**
Check with your vendor.

Are you finding access is slowed down through devices that need additional software to authenticate a user?

□ **Yes**
You might want to add cloud filtering to some / all aspects of your network.

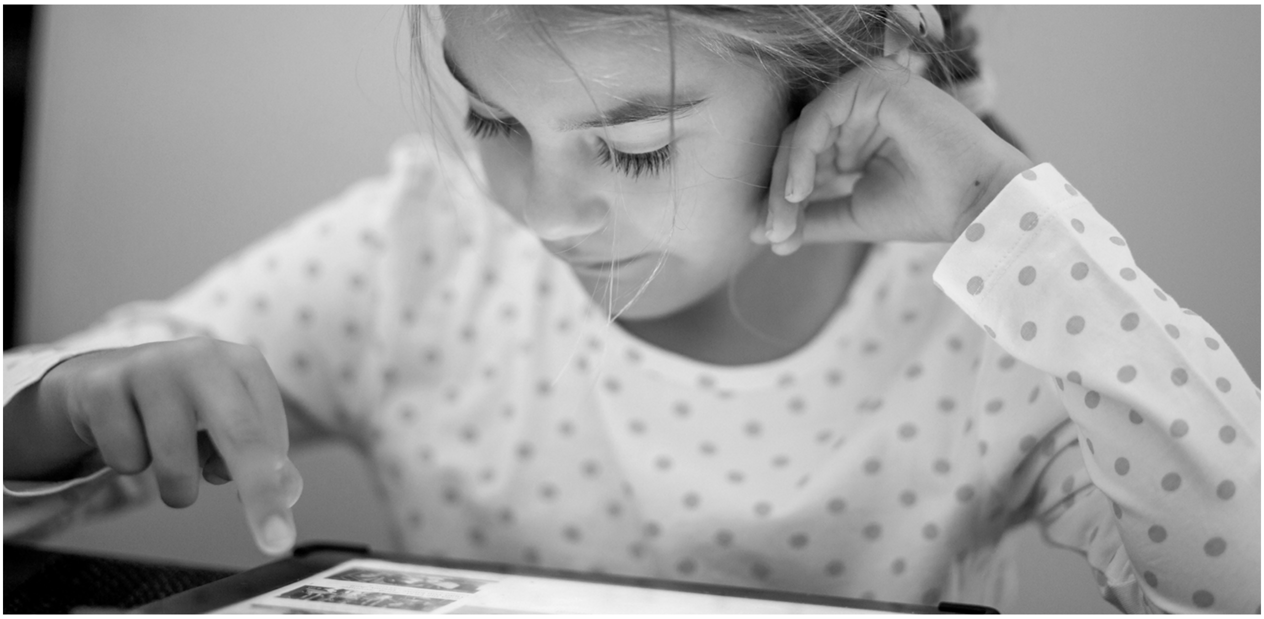
□ **No**
No action needed.

Computer and device check test

Carrying out a practical check can help you to see if your filtering is working to the level you expect. Below are some tests you might want to try.

We would recommend you do this in collaboration with your IT colleagues.

- Try a Google search exploring websites about self-harm. See if you are allowed access to any. □
- See if your system is allowing you to allocate your bandwidth effectively so that high usage areas such as media and file-sharing are controlled. □
- Search YouTube for an age restricted violent gameplay video and see if it is accessible. □
- See if you are able to access the network through a VPN. If you do not know a VPN they can easily be found by googling 'VPN'. □



Section 2. Digital Monitoring

2.1 What is digital monitoring?

At its most basic level, monitoring can simply be the eyes and ears of a teacher. Although human vigilance is crucial, it identifies only what is visible or spoken about.

Digital monitoring is an alert system for uncovering issues you might not have noticed in your students through their classroom behaviour. It can help to uncover and prevent issues such as mental health, drugs, exploitation, radicalisation, gang activity, violence, bullying and self-harm.

Smoothwall's own research has shown that while 95% of teachers rely on a student to tell them if they are being cyberbullied for example, only 5% of students said they would ever confide in a teacher. That's an alarming disconnect. And that's where digital monitoring comes in.

KCSIE and Ofsted believe appropriate monitoring is an essential part of keeping your students safe. It is not possible to successfully safeguard your school without good monitoring.

How it works
Unlike filtering, monitoring doesn't block content. It sits in the background on a computer and will take a silent screenshot if any word or phrase regarded as 'risk' is typed into a keyboard.

That happens whether the word or phrase is typed into a Word document (even if it's quickly deleted and not saved, and even if it's white text on a white background), a browser, a social media site, or an encrypted app such as WhatsApp.

The screen shot is then risk analysed usually on a scale of 1 to 5 so that appropriate intervention can take place if needed.

95% of teachers rely on students to tell them if they are being cyberbullied. Only 5% of children say they will confide in a teacher. That’s an alarming disconnect.

Smoothwall Insights, 2018.

There are generally two types of digital monitoring.

Self-service
In a self-service solution, the risk analysis is done by the DSL. The DSL will scroll through the captures once or several times a day to determine where help might be needed.

The downside to self-service is time. It can be very time consuming to scroll through every capture. For those DSLs who have other responsibilities this could result in a high or severe risk going unnoticed until it's too late.

Moderated or Managed Service
In a managed service, sometimes referred to as a moderated service, the analysis is done by artificial intelligence and then again by a team of external human moderators. Low risks are viewable in the Software Dashboard by the DSL to review every few days. When a higher risk is recorded the DSL is notified immediately by email and by phone.

This is a more expensive solution but gives more peace of mind to DSLs – particularly those with multiple job roles, and less time.

Data privacy
Responsible monitoring set-ups include the use of an acceptable use policy so that clear digital guidelines can be set out for students and their parents.

With the right set-up, digital monitoring ensures that all risk activity is recorded and accessible by safeguarding staff. Any other activity is not recorded and remains private.

Impact on lessons
Digital monitoring has no impact on lessons whatsoever. Nor does it affect your network speed.

2.2 Key terms unpicked

The key terms around monitoring are below

Digital monitoring in real-time
Real-time means the screenshot is immediately available to the DSL or moderators with no delay.

If a student is planning a drug-exchange, about to commit a violent act, or is looking at websites related to suicide, DSLs need to attend to these situations immediately.

Real-time functionality can mean the difference between a successful or unsuccessful intervention.

Auto pre-grading
Auto pre-grading is the term used to describe a self-service monitoring function that pre-grades the concerns raised.

The solution separates alerts into categories and informs a DSL of the severity of the alert. This is useful in helping the DSL to organise concerns in order of priority.

System interface
In self-service monitoring, the system interface is the environment or dashboard used to check monitoring activity. This is one of the most important aspects to consider when evaluating which monitoring solution to use.

Some monitoring solutions may only provide a limited representation of alerts, some may even simply provide a list of internet logs created.

A good interface will allow you to view alerts quickly, focus on individual students easily, and be intuitive so that you can instantly see the severity of all alerts received and be able to check for trends in behaviour amongst your cohorts.

Out of browser monitoring
This refers to digital activity that happens outside of an internet browser.

It can include MS Word, online chats, email or encrypted apps such as WhatsApp. It's important that out of browser monitoring is included in your solution.

Customisation
Customisation refers to additional words you want to monitor.

This is particularly helpful for coded words students may use to talk about drugs for example. Or any type of local slang.

2.3 Knowing the best monitoring fit for your school/college

When purchasing your monitoring solution, your IT colleagues will likely have considered a number of factors. The table below explains what these are so you can better understand the decision they made.

	Benefits	Drawbacks	Best fit
Managed monitoring	DSLs have peace of mind that the school devices are being monitored at all times. Reduces the number of false positives to a minimal level making sure that all alerts are easily managed.	There may be some limits to intricate customisation.	Schools with busy DSLs and large numbers of alerts that have to be managed.
Self-service monitoring	Can keep all alerts and data on-site.	DSLs may have many alerts to manage. Can be time consuming for DSLs to searc through alerts.	Schools that have the safeguarding staff capacity to manage all the alerts created and ensure nothing is missed.
Out of browser	Applications used offline including instant chat, email and MS Word will be fully monitored.	May not be required for young children	Schools in which supervision of digital devices can be stretched due to class sizes of 15+ and students having access to devices outside of lessons.
Customisation	You can add school specific keywords / settings that are specific to your school.	Will need technical input.	Schools that want to personalise their monitoring to their individual needs.

	Benefits	Drawbacks	Best fit
Keystrokes	Can monitor everything typed on a device.	None.	Schools that want all devices monitored for anything typed by a student.
Pre-grading	Can keep all alerts and data on-site.	None.	Schools that need to see how urgent an alert is and can be more guided in how swiftly they need to react to a concern.
Intuitive interface	Applications used offline including instant chat, email and MS Word will be fully monitored.	None.	Schools that have more than 150 pupils so that trends can be analysed and alerts managed more easily.

2.4 Reviewing your monitoring

If you are already using digital monitoring below are a few useful questions to ask IT colleagues to better understand the level of protection you have in place.

Tick a box to highlight any points you wish to follow up on.

Does your monitoring provider protect your data privacy?

□ **Yes** The school providers have supplied privacy statements or security certificates to assure you that all data is kept at maximum security.

□ **No** You should consider what sensitive data could be at risk and consider whether you should change to a more secure provider.

□ **Unsure** Check with your provider.

Are monitoring alerts coming through in enough time for us to be able to deal with a concern?

□ **Yes** Effective, no need to review.

□ **No** If you are not informed of issues quickly enough, you may miss vital information to enable you to act on an immediate urgent risk concern.

Are the monitoring alerts we receive providing enough information? Are we able to access the full contextual evidence of an incident?

□ **Yes** You can see a full context and are able to see whether an intervention is needed. No need to review.

□ **No** You may want to add to query further. Information is only helpful if you can act upon it.

Does our monitoring pick up emails that look suspicious?

□ **Yes** No need to review.

□ **No** Your emails are not monitored. You may wish to review.

Computer and device check test

Carrying out a practical check can help you to see if your monitoring is working to the level you expect. Below are some tests you might want to try.

We would recommend you do this in collaboration with your IT colleagues.

- If you are allowed access, check whether an alert is sent through your monitoring system. Look at what the alert tells you. Are you given enough detail to be able to approach a student knowing what activity has actually taken place? □
- If you are able to access the internet through the use of a VPN, check that your monitoring will pick up any problematic behaviour by visiting a trigger such as searching for knives and blades. □
- Try logging in as two test students at once and using a collaborative document. Write something you would expect to create an alert. Check that your online monitoring picks this up as a high urgent risk. See what information the alert will give you. □
- Try sending an email using the student test accounts and send an email asking one of the students to meet but ‘don’t tell your parents”. See if this triggers a monitoring alert as a child at risk. See what information the alert will give you. □

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, record keeping provision and e-safety training work in tandem to keep young people safe and your organisation compliant with the legislation, guidelines and recommendations placed upon it.

Our partners

Smoothwall are members of the Internet Watch Foundation (IWF) and implement the Child Abuse Image Content list of domains and URLs. Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. We are partners to EduGeek and regularly consult Headteachers, Teachers, DSLs, IT leaders and a range of supporting bodies across UK Education.

About The Key

The pace of change in education means there is no shortage of theory, opinion and advice on what leaders need to do and what they need to know. Leaders themselves are under huge pressure to make a difference with little time to plan, prioritise and learn.

In a world like this, ambitious and aspiring education leaders are in constant need of reliable, relevant and authoritative knowledge that's ready to use.

The Key cuts through the noise to provide up-to-the-minute sector intelligence and resources that empower education leaders with the knowledge to act. Our vision is to be an indispensable partner to education leaders determined to make a difference.

Our services

The Key for School Leaders - Authoritative knowledge for school leaders who are making a difference. Anytime, anywhere.

The Key for School Governors - Governance know-how to help you make a difference to your school.

The Key for Trust Leaders - Authoritative and practical MAT leadership know-how.

CPD Toolkit - Eliminate the hassle and expense of sending staff to external training courses.

Compliance Tracker - The easier, more efficient way to track and monitor your school's compliance.

Safeguarding Training Centre - Keep your pupils safe with effective and reliable staff training.

ScholarPack – the only MIS created especially for primary schools.

The Key

Get in touch

For more information about The Key, our services or to become a member please visit www.thekeysupport.com

Tel: +44 (0)800 061 4500
Email: enquiries@thekeysupport.com
Twitter: @thekeysl

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