Digital Safety

Web Filtering and Monitoring

How to Scale Across a Multi-Academy Trust

A guide for IT leaders.

Practical insights for achieving best practice at the lowest cost.

Whitepaper

Contents

About This Document

When it comes to digital safeguarding IT Leaders in Multi-Academy Trusts face 2 unique challenges.

How to scale their safeguard technologies and how to do it cost-efficiently.

There are 7 factors which can help you address both.

1. Standardisation
2. Onboarding new academies
3. Choosing the right deployment strategy
4. Thinking beyond filtering
5. Evaluating artificial intelligence
6. Know your statutory obligations
7. Point products, or a safeguarding suite?

This document examines each in turn and provide a practical reference guide to help IT Leaders standardise, scale, save money and build more efficient ways of working.

Essential reading for:

IT leaders, their teams and anyone responsible for digital safeguard technology within a multi-academy trust.

If you have any questions about your online safety solutions or online safety in general, 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®

1. Factors at a Glance

1. Standardisation

Standardising filter policies is the cornerstone to consistent safety levels and more efficient working. How can you approach it?

2. Onboarding new academies

MATs are routinely expected to onboard new sites, which may be geographically distant, and have dissimilar processes and systems. How does the IT leader join these new organisations into an already complicated Trust without compromising safeguarding?

3. Choosing the right deployment strategy

Historically, on-premise filtering has been the norm in UK education. More recently alternative hybrid arrangements or even pure cloud filters are coming to the market. The forward-thinking Trust is exploring all options and understanding the best strategy for them. Which will work best for you?

4. Thinking beyond filtering

These days, digital safeguarding is more than filtering. Digital monitoring, record keeping, and classroom management technologies are now common components in a digital safety infrastructure. Many of these systems, however, are designed to operate in a single school. How can you ensure a consistent, cost-effective plan to work across the entire Trust?

5. Evaluating Artificial Intelligence

Most education filters employ AI, but do they do the same job? What does this mean for the Trust, and is it possible to understand what good looks like from the outside?

6. Know your statutory obligations

Safeguarding regulations are updated with reassuring regularity. At the same time, it's not easy to keep up with the ever changing rules. What applies to you and what should you leave aside?

7. Point products, or a safeguarding suite?

Should you buy a stand-alone filter, a filter bundled with DLP or Malware sandboxing, or should you opt for filter that's part of an EdTech suite? What's the difference and how do you know what's right for your Trust?

2. Standardisation

Bringing existing schools into the fold of a Multi-Academy Trusts brings several technological challenges:

i. How to implement the Trust's standard technology practices in schools who already have their own established infrastructure, policies, knowledge and expectations.

ii. How to deal with existing school technology that may conflict with the Trust's own standards.

iii. How to design and implement policies and systems for schools that may be spread over different geographies and demographics.

iv. How to make a significant organisational and technological change as simple and pain-free as possible.

When you design, implement and refine your web filtering policies there are clear benefits to having a standard Trust-wide policy; it's easier to troubleshoot, there are lower maintenance costs and there will be more consistent results in each Academy.

A web filter should be able to manage a shared policy across all Academies, distributed from a central location. This ensures that all sites have the same base policy. The rules contained in this policy may include standard categories for unacceptable content, plus different rules for staff and students, and then based on year group, subject and safeguarding risk.

As well as distributing category rules, standardisation should also apply to custom defined categories, such as URL/Domain allow/block lists maintained by the Trust.

This ensures that, for example, any rules required to bypass filtering for certain applications are applied Trust-wide.

Directory and group management

It's not uncommon for Trusts to want to manage a central directory service for all users. This might be with Microsoft Active Directory, Google GSuite or similar.

However merging an existing school directory into the central Trust directory can be a significant undertaking. It's key to ensure that the web filter integrates with both the central Trust directory and any individual Academy directories.

Mapping

Once integrated, a mapping can be created in the filter that associates the group "Students" with both the student groups from the central directory and the individual Academy directories.

It is then possible to create policies based on group membership Trust-wide.

For example, blocking access to online games for all students during the school day.

This consistency and standardisation across the Trust is essential to having a scalable operating model.

Object-based management

Even with centralised policies you may find subtle differences between academies that your filter finds difficult to manage.

A web filter that uses object-based management with a flexible policy methodology can help simplify this.

In the aforementioned example of blocking certain categories during the school day, this can be complicated by different sites having different school hours.

A filter with object management can use the same 'blocking' object (list of categories/domains) but different time objects for each Academy. Therefore only the blocking object needs to be updated to change the categories for all schools.

Who	What	Where	When	Action
Year 7 students	Year 7 blocked categories	Baker Street Academy	Baker Street - School day	Block
Year 7 students	Year 7 blocked categories	Holmes Academy	Holmes - School day	Block
Year 7 students	Year 7 blocked categories	Watson Academy	Watson - School day	Block

Local control

Prior to joining your MAT individual schools will have managed their own filtering. Often they expect to retain some level of control, particularly in rule management and reporting.

The filter should allow them to make changes to certain parts of the filtering without being able to override core Trust rules.

For example, the ability to allow or block individual sites without permitting access to adult and illegal content.

To ease the burden on central IT, It's a good idea to allow the filter reporting system to allow authorised Academy staff to run their own reports. These can be limited to just the data from their own Academy.

3. Onboarding New Academies

It can be challenging to change the tools and processes of an incoming academy to those used by the MAT. Users have emotional investment in existing tools, schools have invested time in configuring their filters and safeguarding systems, and there can often be a large financial penalty for moving an in-life contract.

These kinds of movements are not as frequent in private companies. But they can happen multiple times a year in education - especially for bigger MATs. And it's showing no signs of slowing. It's not uncommon for schools to onboard with one MAT and then transition to another.

Training

Managing the human element in switching systems can be difficult to get right. Local IT power users may be ingrained in their use of different software. And in safeguarding particularly, a change can be seen as a big problem.

The best way to alleviate the pain is to train new users in your preferred systems. IT users will feel much happier when they are experts in the new system, and can answer their users' questions with confidence.

Those responsible for safeguarding will likely feel more comfortable when they know that everything in their old process maps neatly to the new. And crucially, that nothing is lost.

They are understandable concerns. Missing a key issue could be life changing or even life threatening to the young person affected, and potentially career limiting to those responsible.

Ensure your that your filter provider can offer training – either on-site or remotely.

Check also that they are willing to re-engage when you add a new site.

Below is a useful schedule to help you plan your training provision

Area	Who to inform	What to cover	Who should cover it?
Filtering	IT team	New user interface, reporting and application of policies	Vendor, local or remote
Filtering	Safeguarding team	What can be reported on, what's being blocked or allowed by the new filter system	Local IT team
Filtering	All staff	Advance warning of changes	Email update or similar
Monitoring	Safeguarding team	New UI, alerting procedure	Vendor, local or remote
Monitoring	IT team	How to install	Vendor documentation
Monitoring	All staff	What's being monitored, and why	Email update or similar
Record keeping	Safeguarding team	New UI, process flow	Vendor, local or remote
Record keeping	All staff	How to report a concern	Training delivered by local Safeguarding team

Configuration management

A filter may work well when used within one organisation, but not so well across multiple sites and with differing organisational structures. Choosing a web filter that handles the latter facilitates new school onboarding with minimal configuration changes.

Check that your configuration system allows for ordered policies enabling you to 'layer' the Trust's policy with that of the new school.

This provides a superset of both and will cater for the transitional period where a new school needs to be up to Trust standard immediately but may need some time to adapt to the changes.

Where possible, the configuration should be manageable centrally. A "master" configuration allows your trust-wide policies to be pushed to all filter units – or, in the case of a central deployment, applied to all tenants. This saves time, and ensures consistency.

Finally, look for a vendor willing to help with translating configurations.

If your new school has a niche system, or something uncommon to education, it may be more difficult to export their filter rules and merge them with yours. An extra source of expertise here can speed up the process.

Contracts and costs

Incoming schools are often under different contracts for their filtering and safeguarding products which can be anything from 3 to 5 years in length.

A single vendor across the Trust for all solutions faciliates technical support and day to day operation. It's the ideal although budgets may not permit changing all systems at once.

What can your vendor do to help?

Some vendors will treat each school as a new sale, and not provide the discount appropriate to the scale of your Trust. Ask your vendors for an option to scale your licence to cover this situation.

Where there is an onerous contract with an incumbent, it's worth asking your preferred vendor if they will acquire that contract in exchange for your business or a longer contract with you. Vendors who are MAT specialists will understand this scenario and may have provisions to help you. Smoothwall offers Optimum which enables you to purchase multiple products at large discounts, as well as take over your existing contracts.

Also if you're planning to bring on extra sites but the plans are still at an early stage, or dates aren't yet finalised, share this information with your vendor. It will help them to help you financially.

Network and connectivity

Bringing a new site on board usually means adding another Internet connection. You may find the new Academy is on the same ISP as the rest of your Trust, but it's rare and there can still be migration difficulties.

Can your filter vendor help?

It may seem like there are advantages to having your ISP and filtering with the same company. In reality, a vendor who is tied to their own connectivity might find it difficult to quickly deliver filtering to your new site.

Much better to choose a vendor and ISP or service partner who work together. This will allow the partner to disaggregate filtering and connectivity, giving you more flexibility in how you roll out to the new site.

Additionally, check if your filtering and safeguarding vendor can offer tactical solutions like an IPSec VPN. This can bridge the gap between the options of waiting until the end of term to align the new site with your MPLS network, or paying more to do it now.

Finally, if your filtering, safeguarding and record keeping products are all capable of cloud deployment, it should be much easier to work around any temporary issues with your network.

Use this checklist to see how well prepared you are for the inevitable new site.

Item	Solution in Place?
Training availability	
Pricing scalability for existing suite	
Contract buy out strategy available?	
Configuration management plan	
Plan to support sites not on MPLS or our WAN	

4. Choosing the Right Deployment Strategy

On-premise, cloud or hybrid?

Deployment options are expanding. Cloud-based web filtering is becoming more common than ever before.

Some MATs have chosen to ditch their on-premise environments altogether. A recent survey of schools by QA Education found that school apps in the cloud will increase from 15% to 73% in the next 3 years[1].

There are, however, valid reasons why you might choose to stay with your traditional on-premise system; which, after all, was the norm in UK education until very recently.

Major technology vendors emphasise the benefits of storing data and running applications, platforms and infrastructure in the cloud - whether public or private. But many education IT leaders, remain caught in the debate over maintaining on-premise systems versus moving to the cloud.

The key thing is to understand the case for each and make an informed decision. Clarity is essential to meeting your safeguarding statutory and organisational obligations.

This section contains a summary of each.

Cloud filtering

Types of cloud filter

DNS filter - Easily deployed but deficient in an education setting, the DNS filter only blocks sites at domain level.

Public cloud pass-through proxy - Increasingly rare in Education, these are traditional proxies which work in public cloud data centres and can suffer from bandwidth tromboning, poor latency performance and high running costs.

Private cloud pass-through proxy - Commonly used by councils or MATs with all academies routing their internet traffic through a small number of central datacentres, these also can suffer from high running costs and complexity to manage.

Client-led cloud filter - Cloud managed, but with much of the heavy lifting done on-device, these filters work best with managed devices and offer none of the drawbacks of earlier types of cloud filtering.

Client-led cloud filter, is generally regarded as a more suitable deployment option for an education setting.

Cloud Filtering enables you to remove filtering from your on-site server and apply it directly to your client machines. This gives you more freedom in how you filter managed devices and is particularly useful when you have devices going off-site. It also gives the benefits of faster internet access and more comprehensive data reporting.

Client-led cloud filtering benefits

- Student safety - It allows you to provide filtering both on and off-site and is less restricted by server dependency. This is particularly useful for 1:1 programmes. Additionally, students tethering devices to hotspots are filtered 100%.
- Fast internet access - It gives pupils and staff fast access on any device. The simplification of authentication of users also makes for a more streamlined process.
- Fast deployment - It removes the need for the installation of complicated hardware, or staff training, to get it on-site and working speedily.
- Lower IT maintenance - With the cloud hosting your filtering maintenance time is reduced, giving valuable hours back to your IT team.
- No capital expenditure - It eliminates the need to purchase and maintain expensive servers upfront. Cloud filtering allows you to subscribe for exactly what you require over time.
- Scalability without new appliances - The cloud is a dynamic solution that allows your MAT to expand or contract quickly, ensuring optimisation for current usage.
- Always latest edition - Cloud filtering will always run the latest version without the need for running updates on servers.
- No bottlenecks avoiding choke points - Cloud filtering happens at device level and so activity is distributed across all devices.
- Security - Data in the cloud is encrypted and held on remote, physically secure sites.
- Back-up of data - Cloud services are much more likely to have easy recovery of any lost data.
- Simplified content filtering - Some solutions allow you to achieve real-time, content aware filtering without the complexity of man-in-the-middle (MitM) decryption, certificates or exceptions.
- Lower energy costs - With no need for high power servers to run, energy bills can reduce.

Traditional on-premise

Most education IT Managers are familiar with installing their web filter in a local rack. In many cases, on-premise systems are easier to modify and an ability to customise to specific needs is important for an organisation.

On-premise web filtering puts more control in your hands up to and including the security of your data. It's therefore essential that your organisation is capable of safeguarding its most sensitive information which can be a frequent target of cyber-criminals.

Filtering on BYOD can often pose an issue for institutions. On-premise delivers the best option for creating effective BYOD functionality.

On the face of it on-premise web filtering may be better suited for larger schools with higher budgets; a desire to customise system operations; and the existing infrastructure to host, maintain and protect its data.

The benefits of on-premise filtering

- **Budgets for improvement** - Your organisation may have separate budgets for significant infrastructure changes. A major on-premise filtering purchase might not have to come from your mainstream IT budget.
- **Cost upfront/subscription** - With most of the cost arising from the initial outlay, institutions that use systems for long periods of time may calculate a smaller overall spend than a regular subscription service.
- **Data security** - Data security remains in the hands of your Trust. This can give peace of mind provided you have adequate protection in place.
- **Customisation** - Deployment may take longer but it allows you to add more customisation to your infrastructure. This can be a benefit if you have large or complex systems.
- **Existing infrastructure** - The DfE advises institutions to review their current infrastructure and existing contracts arefully to make sure introducing cloud will not result in a duplication of cost.

Hybrid Deployment

While the debate of the pros and cons of an on-premise environment pitted against a cloud computing environment is a real one, there is another model that can offer the best of both worlds.

A hybrid solution features elements of both on-premise and cloud, and can leverage the benefits of both.

Usually such a deployment retains a less powerful hardware appliance on-site and is combined with client deployment for a proportion of student systems. Sometimes these deployments start heavily skewed towards the existing on-premise solution where an organisation is migrating to a more balanced hybrid setup.

How might a hybrid deployment work for filtering?

A hybrid solution can be the best solution if you are concerned about any of the following:

- Load distribution - As internet traffic increases, the need for powerful filter hardware can arise. With bandwidth ever cheaper, it can prove expensive to keep up. Cloud filtering can alleviate the bottleneck at the gateway edge and extend the capability of more modest hardware.
- Authentication - By introducing the cloud solution for some devices, you can remove the need for additional authentication methods, particularly for modern devices such as Chromebooks, improving the accuracy of filtering and logging, and ultimately improving safeguarding outcomes.
- Managed devices off-site - There is a growing need to filter managed devices off-site. If that applies to you and you wish to still retain your on-premise filtering model, a hybrid solution will allow you to add a cloud solution to all devices that go off-site and may be an ideal option.
- Flexibility - A hybrid solution can provide your institution with the flexibility to match evolving needs. For example, you may wish to choose how to distribute depending on available resources. Or you may be planning to roll out programs such as 1:1 which will involve adding more devices over time. Hybrid can be ideal for meeting flexible and changing requirements.
- BYOD - Some institutions require the benefits of cloud but also want the most effective filtering for BYOD. Hybrid allows you to achieve both scenarios.

5. Thinking Beyond Filtering

These days, digital safeguarding is more than filtering.

Digital monitoring, record keeping, and classroom management technologies are now common components in a high quality, digital safety infrastructure.

Active monitoring tools such as Smoothwall Monitor constantly observe digital devices to check for signs of risk to children. Record keeping systems such as Safeguard Record Manager allow both online and offline safeguarding incidents to be logged and tracked within an individual pupil's safeguarding chronology. This allows the DSL to record how they manage incidents, escalate to authorities if required and ensure their organisation fulfils its statutory duty of care.

Moderation

Active monitoring tools are typically installed on each device within a school. They work by recording activity and reporting suspicious events to a Monitoring server – which is often a Cloud-based service. These services will record each event that triggers certain categories using tools such as machine learning and artificial intelligence.

Automated analysis tools will never be 100% accurate, which is why events need to be moderated by a human – particularly for events that may indicate a high risk to safety or even life.

Human moderation is performed either by the school's own staff, by a person within the Trust or by the monitoring provider.

Unless the MAT is very large, it is unlikely to be in a position to dedicate a full-time person to review safeguarding events. Using the provider's own managed monitoring service can be cost effective and an easy way to scale the service.

This also leverages the provider's scale and experience to deliver a reliable service – often during out-of-hours and holidays too, which is vital for MATs who have take-home devices for students.

Hierarchies

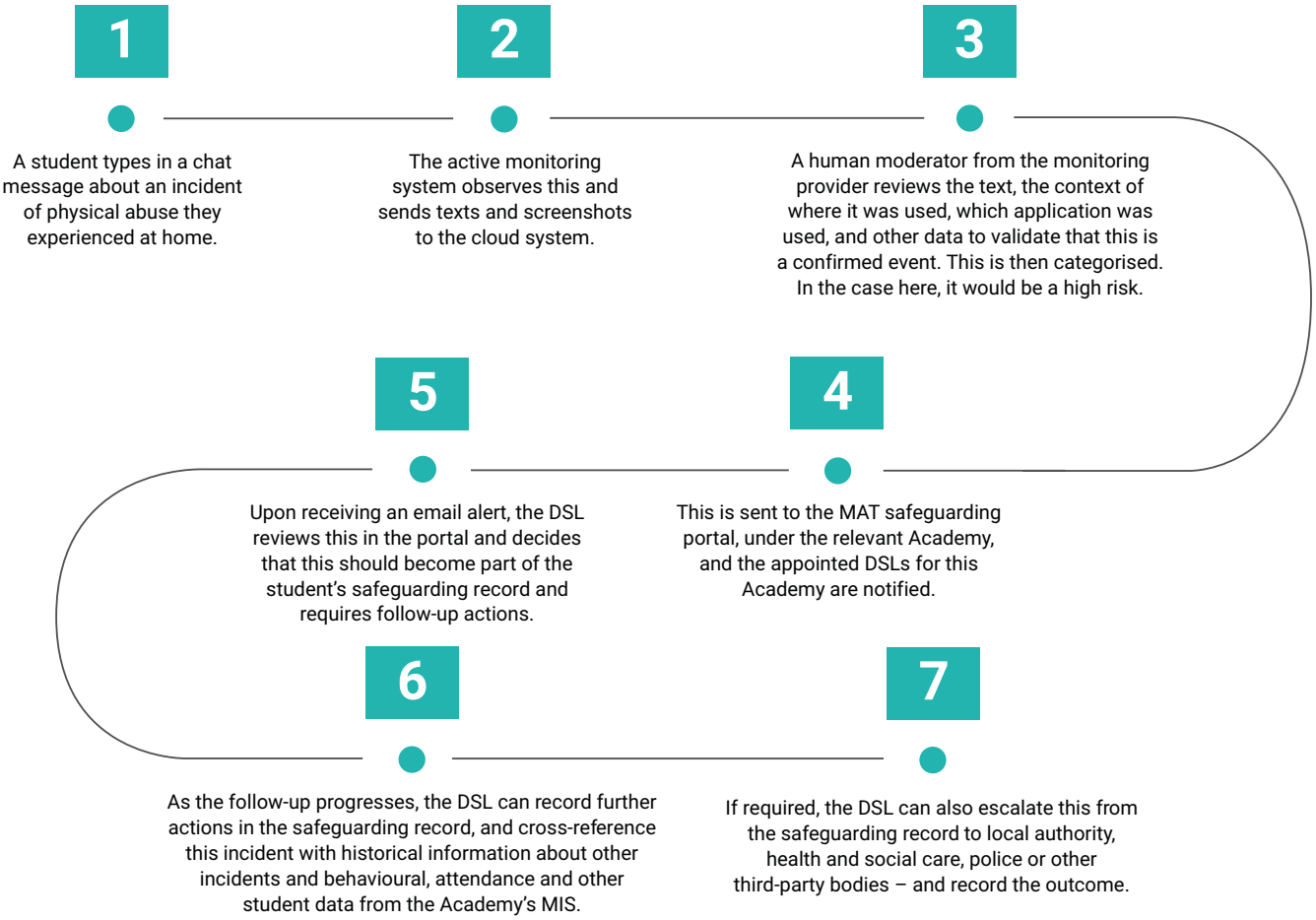
MATs may often have a Trust-wide safeguarding officer who is responsible for all academies. It is essential that all safeguarding leaders understand the structure of a MAT - so that they can themselves help respond to events, observe performance of the individual academy DSLs, and ensure consistency in the Trust's approach to safeguarding.

A hierarchy in the system – with the MAT as the 'parent' and individual academies as 'children' - allow appropriately trained safeguarding staff at the Trust-level to view and manage information at all levels.

This avoids the security challenges of managing individual logins for each academy. It also provides Trust-wide reporting, without having to manually aggregate data from individual Academy reports.

Integrated Solutions

For an incident to be tracked end-to-end, an active monitoring tool should integrate with the record keeping tool. And the record keeping tool should integrate with the school's MIS, for pupil information.



An integrated process with systems connected and aligned is key to scaling. Policies, procedures, tools, systems and training materials can be common across the MAT – helping provide a consistently high level of care in a cost-effective way.

6. Evaluating Artificial Intelligence

These days it's unusual to find a web filter vendor not making use of machine learning or intelligence somewhere in their products.

But what do they do? And how can you differentiate good from not so good?

Artificial Intelligence (AI) 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 is attached to the URL. The categorisation makes it back to the point of filtering in regular URL list updates.

7. Know Your Statutory Obligations

With the online space constantly evolving, Ofsted and statutory guidance are continually being updated. It can be a challenge to keep up. But a failure to do so can endanger student safety and compromise your Trust's reputation.

Below is a handy refresh of the key points.

KCSIE 2019 Statutory Guidance[2]

The online aspects of KCSIE guidance look to ensure schools see online safety as a safeguarding risk. It wants schools to be aware of the safeguarding issues to look out for and to follow concerns up effectively:

- Proprietors and school governance should "ensure appropriate filters and appropriate monitoring systems are in place" but should avoid "over-blocking" so that learning isn't restricted.
- A Designated Safeguarding Lead (DSL) should take responsibility for online safety in school.
- Students should be taught about safeguarding "including online safety".
- Staff should be aware of the types of safeguarding issues to look for.
- Clear record keeping is crucial for best practice in safeguarding.

The Prevent duty[3]

Prevent is a legal duty to ensure students are not drawn into extremism and came from the 2015 Counter-Terrorism and Security Act.

- All schools must legally protect students from access to "terrorist and extremist material" through "appropriate levels of filtering".

Ofsted 2019[4]

Ofsted mirrors the KCSIE legislation. It provides details of the types of risks that need to be identified and what inspectors will look for:

- Leaders should "oversee the safe use of technology" for learners in their care and act "immediately if they are concerned about bullying or children's well-being".
- "Appropriate filtering and monitoring are in place."
- All staff must "understand the risks posed by adults or learners who use technology, including the internet, to bully, groom, radicalise or abuse children or learners".
- Schools should protect against online bullying, discrimination, extremism, child exploitation, and county lines.
- Leaders and staff ensure protection while enabling students "age-appropriate and reasonable risks."
- Inspectors will explore how schools "educate pupils in online safety and how the provider or school deals with issues when they arise."
- Safeguarding records are up to date and concerns shared appropriately.

UK Safer Internet Centre (guidance linked in KCSIE 2019)[5]

The UK Safer Internet Centre provide helpful advice in the way effective filtering and monitoring should look. The KCSIE legislation links to this guidance.

Key aspects include:

Overall: An online safety risk assessment should take place annually.

Filtering

- Schools should ensure that all illegal content is blocked.
- Inappropriate content is managed including: discrimination, substance abuse, extremism, malware, pornography, piracy and copyright theft, self-harm and violence.
- Schools are advised to use filtering that can: differentiate by age, identify users, filter mobile and app content, and have a clear reporting system.

Monitoring

- Monitoring should be used to "safeguard children and the responsibility therefore should lie with the school leadership/governors and designated safeguarding lead".
- Monitoring should identify: accessing illegal materials, bullying, child sexual exploitation, discrimination, substance abuse, extremism, self-harm, pornography, violence and suicide.
- Active/proactive monitoring can "prove particularly effective in drawing attention to concerning behaviours, communications or access".

Ofsted summary value evaluations[6]

- New summary evaluations will take place after a "batched" inspection of academies across your trust. An effective online safeguarding infrastructure will highlight to Ofsted how the Trust ensures outstanding online safety is implemented across the MAT.

8. Point Products, or a Safeguarding Suite?

Today's education 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 safeguarding solutions and there can be cost savings by purchasing this way. Smoothwall offers significant savings for example when purchasing multiple products **www.smoothwall.com/optimum/**

If it doesn't, it's important to consider the other products your filter must work closely with in order to be effective. A failure to properly consider these alignments can waste valuable time and money.

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 on 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 are listed below:

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 a MAT environment.

Our expertise and pioneering solutions make us the ideal choice for expanding Trusts requiring a credible and MAT focused safeguarding provider.

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/mat-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.

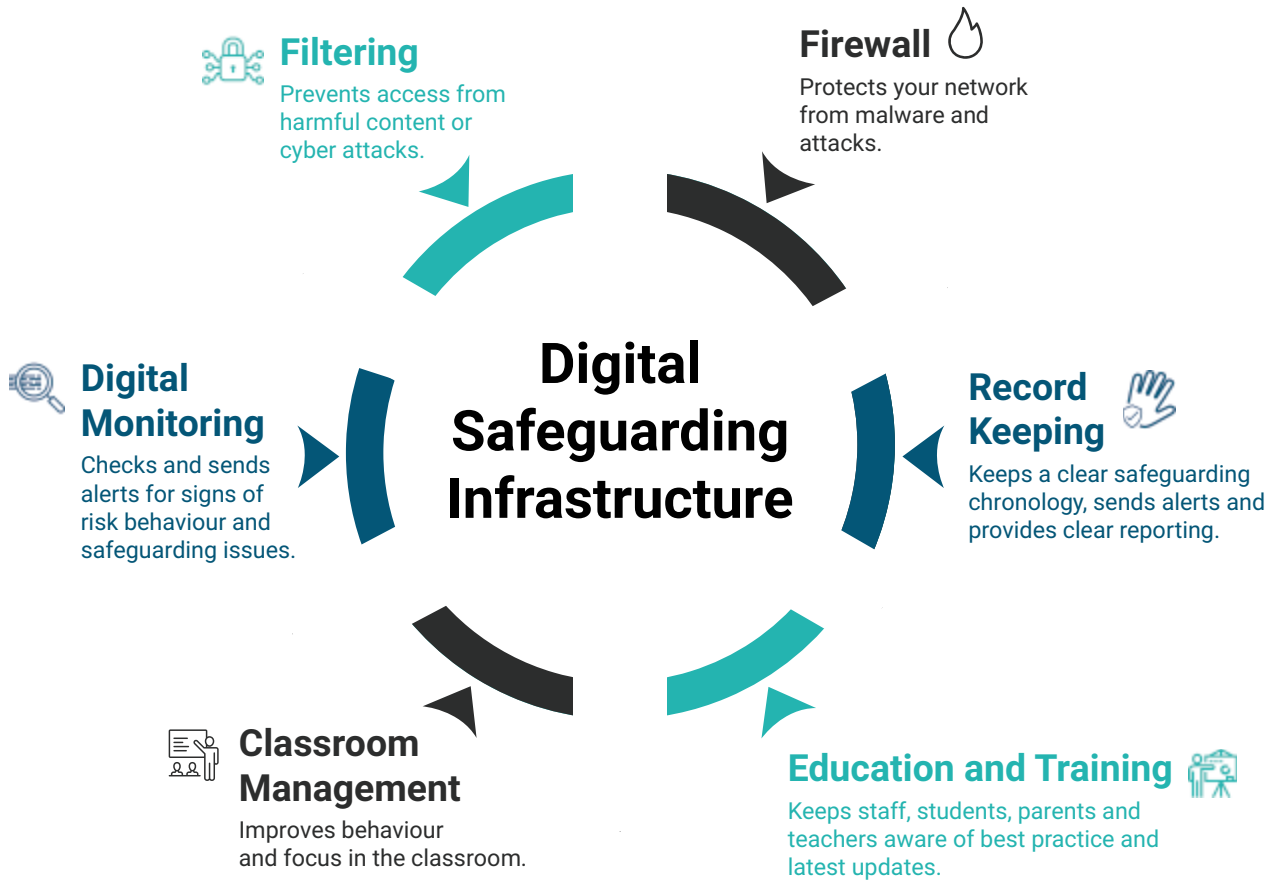
The demands placed on the physical eyes and ears of teachers far exceed their ability to identify all but the most obvious risks, and puts the organisation at odds with both student needs and statutory guidelines.

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.



References

1. QA Education. 2017. https://www.qaeducation.co.uk/content/uk-schools-move-cloud-services-reduce-costs-and-better-manage-their-budgets-survey-reveals

2.Gov.UK. 2018. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

3. Gov.UK. 2019. https://www.gov.uk/government/publications/prevent-duty-guidance

4. Ofsted. 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/769153/Summary_evaluations_of_multi-academy_trusts_070119.pdf

5. UK Safer Internet Centre. 2019. https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

6. Department for Education. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/576240/Multi-academy_trusts_good_practice_guidance_and_expectations_for_growth.pdf

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®