Web Filtering in Education

Cloud, On-premise or Hybrid?

A complete guide to choosing the right deployment strategy for your school or college

smoothwall® by Qoria

Whitepaper

Contents

1.0 Introduction

Our aim in this paper is to give you a better understanding of the deployment options around web filtering and to achieve a more informed allocation of resources. We expand on the on-premise versus cloud debate and share perspectives on why some school IT leaders are choosing to follow a hybrid model where on-premise and cloud computing coexists.

Essential reading for: IT/ Network Managers and technicians working within UK schools and colleges. Also, Headteachers and DSLs wanting a more practical understanding of their IT environments as it relates to safeguarding.

If you have any questions about web filtering, its implementation or digital safeguarding in general, please do not hesitate to contact the Smoothwall team.

We'd be happy to help.

Tel: +44(0) 800 047 8191
Email: enquiries@smoothwall.com
Web: www.smoothwall.com/contact

smoothwall® by Qoria

2.0 The Changing Face of Web Filter Deployment

The online world in education is rapidly developing. Deployment options are expanding and cloud-based web filtering is becoming more common than ever before. Indeed, many schools have chosen to ditch their on-premise environments altogether.

There are, however, valid reasons why a school or college might choose to stay with their 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 IT leaders, including school Network Managers, remain caught in the debate over maintaining on-premise data centres versus moving to the cloud.

With restricted budgets and often complex requirements, keeping up with ever changing technology can seem challenging for schools and colleges but it's essential in order to meet many of your statutory and organisational obligations, especially around safeguarding.

With restricted budgets and often complex requirements, keeping up with changing technology can seem challenging. But it's essential in order to meet your statutory obligations around safeguarding.

2.1 Web filtering in the cloud

Types of cloud filter

DNS filter – Easily deployed but deficient in an education setting, the DNS filter can block 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.

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.

This report will focus on the client-led cloud filter, as it's 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.

Cloud filtering has many benefits to suit your school or college's needs:

- **Student safety** - 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 investigative reporting** - Cloud provides faster reporting than on-premise solutions as it eliminates the need for an appliance to process large volumes of data. Faster reporting means faster follow up on issues.
- **Fast internet access** - Gives pupils and staff fast access on any device. The simplification of authentication of users also makes for a more streamlined process.
- **Fast deployment** - 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** - 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 school or college 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.

2.2 Traditional on-premise

Most education IT Managers are familiar with installing their web filter on their school or college's own computers and servers. 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 school or college. 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 benefit you if your school or college has large or complex systems.
- **Existing infrastructure** - The DfE advises institutions to review their current infrastructure and existing contracts carefully to make sure introducing cloud will not result in a duplication of cost.

  "Perfectly workable local solutions should not be retired before their natural end of life".
- **Being ready** - Big changes to infrastructure and systems can be another upheaval in times of other change. It may not be the right time for your school or college to consider a complete systems overhaul.
- **Extra training of staff** - Existing IT staff will need to understand the system changes for moving over to cloud. This will involve extra training and may require extra support initially.
- **BYOD & unmanaged devices** - On-premise can be the best solution for protecting on-site BYOD devices. Additionally, other unmanaged devices are easily handled at the network level.
- **Control** - Your school or college may want to retain total control over your filtering set-up.
- **Consolidation** - Filter appliances might double up as firewalls, saving money, and maintaining the same consumption power, cooling and rack space.
- **Assured filtering** - With a filter inline on your network, it's much more difficult for a device to escape filtering, whether it's by mistake or through nefarious means.

2.3 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.

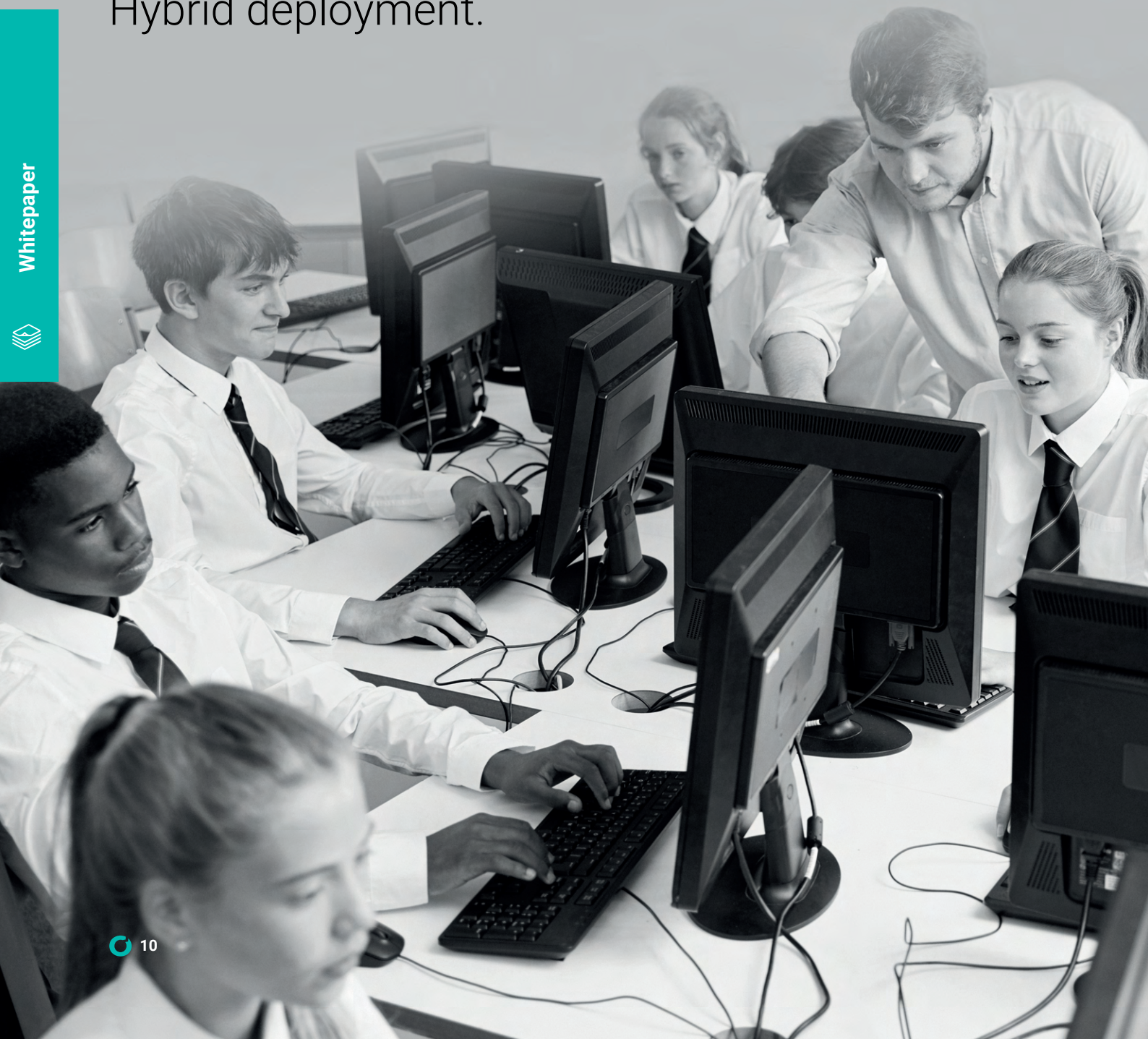
Usually such a deployment retains a less powerful hardware appliance on-site and is combined with client deployment for a proportion of student systems. Sometimes these deployments start heavily skewed towards the existing on-premise solution where an organisation is migrating to a more balanced hybrid setup. On-premise systems are generally considered a capital expenditure whereas cloud-based systems are typically considered an operating expenditure.

How might a hybrid deployment work for filtering?

A hybrid solution can be the best solution for some schools and colleges 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 for schools and colleges to filter managed school 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 a school or college 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 schools and colleges require the benefits of cloud but also want the most effective filtering for BYOD. Hybrid allows you to achieve both scenarios.

While the debate of an on-premise or cloud environment is a real one, there is another model that can offer the best of both worlds - Hybrid deployment.



3.0 Statutory Requirements & Guidelines

When reviewing your filtering arrangements for your School or College it is a good idea to revisit the statutory requirements and guidelines to ensure you are up to date.

The Keeping Children Safe in Education (KCSIE) statutory document[1] explains that:

- *Schools and colleges are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"*
- *Filtering should be "appropriate" for the individual school or college's needs.*
- *Overblocking should not lead to "unreasonable restrictions" as to what children can be taught with regard to online teaching and safeguarding.*

These requirements make it clear that whilst it is essential for schools and colleges to create optimum protection from the safeguarding and security risks that the internet exposes, there is an expectation for establishments to ensure that their filtering provides a granular approach that allows appropriate access whilst also not enforcing unreasonable restrictions.

UK Safer Internet Centre

KCSIE points to the UK Safer Internet Centre[2] for schools and colleges to refer to when choosing their filtering solution. Within this guidance it is suggested that all schools and colleges should have effective monitoring that identifies both illegal and inappropriate content.

The definitions for measurement include :

Illegal online content

- **Illegal images** - Providers should be members of the Internet Watch Foundation (IWF). Access is blocked to illegal Child Sexual Abuse Material (CSAM)
- **Unlawful terrorist content** - Providers should Integrate the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Inappropriate online content

- Discrimination: Any form of unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.
- Drugs / substance abuse: Anyone displaying or promoting illegal use of drugs or substances.
- Extremism: Anyone promoting terrorism and terrorist ideologies, violence or intolerance.
- Malware / hacking: Anyone who promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
- Pornography: Displays of sexual acts or explicit images.
- Piracy and copyright theft: Illegal provision of copyrighted material.
- Self-harm: Promotion or display of deliberate self-harm (including suicide and eating disorders).
- Violence: Any display or promotion of the use of physical force intended to hurt or kill.

[1] Keeping Children Safe in Education 2023. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[2] UK Safer Internet Centre. 2023. https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering

Key features

The UK Safer Internet Centre suggests a solution should meet the following:

Context appropriate differentiated filtering	Can the provider supply a granular solution that allows you to vary filtering strength appropriate to age, vulnerability and risk of harm?
Control	Does the solution have the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Can any changes to the filter system be logged and enable an audit trail that ensures transparency and that individuals are not able to make unilateral changes?
Circumvention	Does the solution have the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS?
Contextual Content Filters	In addition to URL or IP based filtering, what extent can content be analysed as it is streamed to the user and blocked. For example, can it contextually analyse text on a page and dynamically filter it?
Filtering policy	Does the provider publish a rationale that details their approach to filtering with categorisation and classification including as well as overblocking?
Group / Multi-site Management	Does the solution have the ability for deployment of central policy and central oversight or dashboard?
Identification	Will your solution allow you to identify users accessing your network?
Mobile and app content	To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)?
Multi-language support	Will the solution cover the relevant languages required for your institute?
Network level	Will the filtering be applied at network level and not be reliant on any software on user devices whilst at school or college?
Remote devices	Does the solution have the ability for remote school/college owned devices to receive the same or equivialent filtering provided in school or college?
Reporting mechanism	Does the solution have the ability to report inappropriate content for access or blocking?
Reports	Can the system offer clear historical information on the websites that users have accessed or attemped to access?
Safe Search	Does the solution have the ability to enforce ‘safe searcg’ when using search engines?

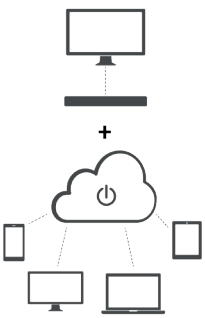
4.0 Choosing The Right Deployment Strategy For Your School/College

With more and more software migrating to the cloud and the clear benefits that brings, a natural progression for many schools will be migrating to cloud filtering or hybrid over the next few years.

That said, on-premise is unlikely to disappear altogether and there are valid reasons why a school/college may wish to stick with their on-premise set up.

4.1 Where are you now in your filtering roadmap?

The following table offers some points to consider when considering your deployment strategy.

Current needs	Possible solution	Solution detail
You are a school/college that has heavily invested in an on-premise solution. You have the staff available to maintain and manage this equipment. You want to have full responsibility over your system and data, you don't mind completing updates on your devices, and do not want to overhaul a system that is mainly reliable with some tweaking.	Traditional: On-premise 	Updating your on-premise solution may be the right place for you now. You're aware that cloud is coming and that you need to move to it in the future, but you would like to wait for cloud filter solutions to be more established.
You are a school/college that has good on-premise equipment but is noticing gaps in some of the filtering requirements you need. You have available staff to maintain the equipment but need to find a solution that will cover these gaps. You need to keep costs to a minimum and need a solution that can cover your changing environment.	Hybrid: Traditional on-premise combined with cloud add-on 	A hybrid solution can allow you to retain your functioning on-premise solution but create an add-on using a cloud solution on top. This can be an easy fix to your situation without having to do a big overhaul of your solution yet. You can gradually progress over to the cloud, giving you time to plan for meeting all your complex requirements through the cloud exclusively. By using a combination of on-premise and the cloud, you will be able to make better cost efficiencies while simplifying management and improving your filtering's overall performance.

Current needs	Possible solution	Solution detail
You want to overhaul your filtering system and bring your school/college fully into the modern IT environment. You don't want to have a huge capital expenditure outlay and are looking for a solution that makes costs more manageable and subscription based. You want to be able to have flexibility in your offering as your device requirements are changing with different numbers of students and ever-increasing devices. You want a no-nonsense solution where your data is protected. You want to reduce the need for running updates to the latest version, freeing you up for the vast amounts of other IT demands that need to be acted upon. You want to avoid bottlenecks with your vast datasets which can be hard on your processors and affect the speed of your reporting. You have overwhelmingly managed devices and no BYOD.	Cloud: Advanced all in the cloud filtering 	Installing a fully cloud-based solution will enable you to create a filtering infrastructure designed for future years. A cloud solution will enable you to manage filtering costs over time without significant upfront expenditure in on-site equipment. The IT infrastructure will be simplified without the need for complicated configuration. The way a cloud solution works will enable you to keep your solution flexible so that you can scale up or change flexibly over time rather than having to plan for all eventualities on day zero. Data in the cloud is normally encrypted and stored in a remote and physically secured site. This is likely more secure than you can achieve on your school or college site. There will be no need for updates as the cloud will automatically run the most current solution. Cloud computing allows filtering to occur at device level and so activity is distributed across every device avoiding bottlenecks.

4.2 Illustrative scenarios

Illustrative scenario A

School of 1300 pupils

300 PCs, 400 iPads

School A would like to simplify filtering on their wireless devices. They find the complexity in on-premise with certificate based MitM filtering causes problems with some key sites and occasional issues with Kerberos authentication. They are reasonably happy with their set-up and have invested in expensive equipment that is working well for them on their windows devices. They have a good level of maintenance available on-site and are just looking for a solution to streamline their wireless filtering.

Solution: Hybrid

The addition of cloud filtering would ease the problems they find, as it uses simplified authentication and no MitM. As they are happy with filtering for their wired computers, using a hybrid solution will improve their filtering service and they can review migrating fully to the cloud in the future.

Illustrative scenario B

College of 3000 pupils

700 PCs

College B have invested heavily in their on-premise filtering equipment. They are currently reasonably happy with their filtering set-up but are wary that with many colleges moving over to the cloud, they will soon be unable to meet the level of filtering required. They have the staff to keep up the essential maintenance but know that the system needs an update. They are wary of overhauling a system that is generally working and don't want to pursue a big change at this time.

Solution: On-premise update

With the right staff in place that are able to maintain an on-premise solution, the college will be able to keep up-to-date by simply updating their appliance-based solution. Although they will not be able to benefit from the benefits cloud computing offers, they will be able to run a fully up-to-date filtering system and be able to review again when cloud solutions are more established.

Illustrative scenario C

School of 1700 pupils

500 PCs, about to introduce 400 Chromebooks with more to be added over following years

School C has a number of wired desktop PCs used by staff and students. However, they are planning to implement a 1:1 strategy and want to be able to achieve fast deployment for these devices while being able to filter the devices on and off-site. They are also looking for flexibility and scalability as they want to trial with their sixth-form before rolling it down to the lower year groups.

Solution: Hybrid or cloud

The school are clearly changing their IT structure significantly. With the plan to roll out 400 managed devices to sixth form, and then to increase this across more of the school over time, cloud filtering would provide the best solution. It will enable the school to achieve fast deployment and easy scalability as the number of devices increase.

Illustrative scenario D

College of 5000 pupils

800 PCs, 100 Macs, 2000 Chromebooks

College D have busy IT staff who are struggling with the time needed to maintain an up to date on-premise filter while having to manage all the other IT needs in the college. They also have vast data sets and are looking to reduce the demand on their processors to improve their reporting. They want to be able to see filtering data over time so that they can gain a full contextual picture of a student when necessary. They have 2000 Chromebooks and need easy deployment and flexibility of filtering on and off-site.

Solution: Cloud

Cloud reporting will reduce the need for staff management and maintenance. The most updated version of filtering will automatically be available without the need for lengthy installation processes. The right cloud solution will also enable them to be able to access a much more comprehensive picture as it will be able to report on 100% of data.

5.0 How to Choose a Vendor

When choosing a vendor, it is important to choose a solution that covers all the requirements as set out in KCSIE and the UK Safer Internet Centre guidance. Looking for a vendor that is established and a specialist in solutions for schools, colleges, trusts and local authorities is a good starting point.

Asking the vendor how they are able to meet the guidelines will give you a good understanding of whether they are aligned with government signposted requirements.

5.1 Checklist of functionality

100% Real-time content analysis	Ensure their solution does not just use a URL block list, but instead uses real-time content analysis to look at pages objectively and avoid unnecessary blocking or missing any pages that should be blocked. For example, a provider that categorises content by analysing the content, context and construction of individual pages is much more effective at finding and blocking inappropriate content without overblocking entire sites. Relying on URL block lists also often means subdomains are not included in the filtering provision – a key and growing concern amongst teachers.
Powerful real-time reporting	Look for a provider that offers timely reporting. There is little point finding out about an incident days after the event.
On/off-site protection	Make sure if you have any managed student devices, you have the option for them to be filtered off-site. Check to see if there is granularity in this.
Full incident reporting	Make sure your provider is able to report on 100% of the data created. This will help build a full contextual picture of an incident.
Authentication	Look for a simple authentication process which makes access smoother and the ability to track all users easier.
Social media controls	Check that the solution gives you options around social media including read-only access.

Data security	Ensure that any vendor understands the specific requirements around school data and has the correct DfE certification.
Easy bandwidth management	Make sure the solution will enable you to control and allocate bandwidth to allow media and file-sharing.
Layer 7 application control	Check the solution will enable you to identify and stop applications you don't want to run on your network and prioritise the ones you do.
Anonymous proxy-blocking	Look for a simple authentication process which makes access smoother and the ability to track all users easier.
Age appropriate	Look for filtering providers that use a wide variety of directories (e.g. Microsoft AD, Google Directory) allowing filtering to be set appropriately at group and user level.
Simplified configuration	Sometimes elements of on-premise solutions can make filtering more complex than it needs to be. Cloud filtering simplifies the approach making filtering easier to configure and less likely to fail. For instance, some cloud filtering solutions are able to analyse content in real-time without the need to add on-premise additions including man-in-the-middle decryption, certificates or exceptions.
Multiple options	Make sure you choose a vendor that can look for a solution that suits you. A good vendor will be able to look at your needs and provide a tailored solution to meet all your requirements. All institutions are different. Some may want a full cloud solution; some may want a hybrid solution.
Deployment	Check that the speed of deployment and the resources you will need on-site match up. Many cloud solutions tend to have a faster set-up than on-premise. Less configuration and equipment on-site often make cloud filtering a speedy process.
Scalability	Check that your solution will easily expand or contract depending on your ever-changing needs. Adaptability is key for a long-term solution.
Vendor reviews	Look for providers that can show you an established history in providing filtering for UK education. Often new players may offer the world as they do not fully understand the needs and challenges of filtering in education and may not be able to deliver what they are promising.
Support	Look for a provider that offers a reliable support service operating in times that suit your time of day.

6.0 Frequently Asked Questions

Why do we need to filter devices off-site?

One of the concerns parents have when schools look to introduce 1:1 programmes are the protection of the devices when they are outside the school. They want you to offer peace of mind that you have the risks covered in and outside of school. Students are more likely to try to take risks outside of the classroom environment.

Will my data be secure in the cloud?

With schools and colleges being vulnerable targets for sensitive data theft, data security is paramount. Most providers using the cloud are likely to suggest that using the cloud is more secure than on-site. Smoothwall uses Microsoft Azure and Google Cloud– some of the most certified and secure datacentres, with tried and tested software.

Is cloud filtering more expensive?

Most cloud filtering solutions will give you a more cost-efficient set-up and allow you to plan for your budget by regular payment options rather than initial large upfront cost. This gives you the flexibility and ease to change your set-up over time.

Is on-premise more customisable?

In complex or large systems, on-premise or hybrid solutions can give institutions more detailed customisation options.

Will a cloud solution be scalable?

One of the main reasons so many solutions are moving to the cloud is the fact that cloud solutions are easy to adapt to your current needs. Many providers operate in bands of users with the possibility to change your band over time.

Will cloud filtering make my old equipment redundant?

Not necessarily. If you have invested in expensive equipment, a hybrid model could add the aspects you currently need without replacing equipment that is working for you.

How quickly can cloud filtering be deployed?

Depending on the provider, most good solutions will significantly reduce the time for deployment from weeks to days.

How can I check that a cloud filtering solution doesn't create over-blocking?

Look for providers that use highly granular categorisation and assess the content of pages. Leading providers like Smoothwall have intelligent rules-based mechanism that allow sites to be more accurately classified and filtered upon, without unduly restricting access.

Have a question that's not answered here?

Contact our web filter experts. We'll be happy to help.

Tel: +44(0) 800 047 8191
Email: enquiries@smoothwall.com
Web: www.smoothwall.com/contact-us

7.0 About Smoothwall Filter

At Smoothwall we know that Multi-Academy Trusts have some important considerations when it comes to digital safeguarding technologies. We know that the internet is now an integral part of school life and that the need for flexibility and mobility of devices is increasing. Varying requirements mean trusts may need a variety of solutions.

We have added Smoothwall Cloud Filter and Hybrid deployment to our on-premise offering, to meet these needs and enable you to take your web filtering to an advanced level. No longer are you restricted to filtering only on-site or the speed in which your filtering can be deployed.

The added benefits that Cloud Filter offers are:

- Filtering devices both on and off-site.

  - Chromebooks with a Chrome extension

  - Windows and Mac with a Chrome/Edge extension and a "companion" agent to handle traffic outside the browser (agent coming early 2024)

  - iPad with a custom browser with filtering built-in, and a companion agent to handle traffic outside this browser

  - Android with a system-level filter for all apps (coming early 2024)

- Cloud managed, all filtering policies and logs are managed from the cloud, automatically synchronising changes to filter clients and on-premise appliances.
- Flexibility and easy scalability so that your needs can be met as they evolve.
- Simpler configuration without the need for man-in-the-middle, certificates or exceptions to use real-time content analysis.
- Logging and reporting of all web traffic meaning that a full contextual picture can be created around incidents.
- Avoiding bandwidth and throughput issues by filtering on the device - with negligible impact on performance.
- Faster installation process and more robust user identification.
- Security of data encrypted within remote, physically secured sites.

Other key elements offered by Smoothwall Filter include:

Real-time dynamic content analysis: Smoothwall provides filtering and reporting that analyses and categorises web content in real-time. This gives schools better protection as URL blocklists often become outdated.

Social media controls: You may want to allow access to social media in your school environment but control how much activity can take place. Smoothwall filtering allows you to have flexible options including creating read-only settings or forcing age-related controls specific to each site.

Anonymous proxy-blocking: When students/staff try to circumvent your filtering by using proxy servers, this can be blocked in real-time.

Appendices

Further reading

You may also wish to download:

Safeguard Monitoring: A Complete Guide to Active Monitoring for Schools

What is monitoring, why do Ofsted require it, and how can you integrate it into a busy safeguarding strategy.

Available at: https://smoothwall.com/active-monitoring-schools

Effective Cloud Filtering in Education

Learn all there is to know about cloud filtering in our comprehensive guide.

Available at: https://www.smoothwall.com/education/effective-cloud-filtering-in-education/

Benchmarking Your Digital Safeguarding: How to Create an Improvement Strategy for Ofsted

A practical guide for school/college Headteachers, Principals, DSLs and anyone responsible for digital safeguarding in an education setting.

Available at: https://smoothwall.com/benchmarking-digital-safeguarding-ofsted

About Smoothwall

Smoothwall is part of Qoria a global technology company dedicated to keeping children safe and well in their digital lives. Over 25,000 schools globally depend on our technologies to provide better student digital safety and wellbeing support.

From 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 and monitoring provision work in tandem to keep your 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.

Smoothwall partners with EduGeek and regularly consult Headteachers, Teachers, DSLs, IT leaders and a range of supporting bodies across UK Education.

Contact us

If you would like an informal discussion about any aspect of your web filtering and its deployment our specialist team are on standby to help.

Arrange a free demonstration

To see a free, no obligation demonstration of Smoothwall Filter, please contact us.

Tel: +44 (0) 800 047 8191
Email: enquiries@smoothwall.com

smoothwall.com

Not ready to renew your web filtering?

Simply send us your name, email and renewal date and we'll contact you nearer the time to discuss your options and provide a comparative quotation.

www.smoothwall.com/contact-us

Smoothwall

Second Floor
2 Whitehall Quay
Leeds
West Yorkshire
LS1 4HR

Tel: +44(0) 800 047 8191
Email: enquiries@smoothwall.com
smoothwall.com

Smoothwall
Smoothwall
Smoothwall-ltd
SmoothwallTV

smoothwall® by Qoria