



Web Filtering for Education

Cloud, On-premise or Hybrid?

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





Contents

1.0 About this document.....3

2.0 The changing face of web filter deployment.....4

3.0 CIPA requirements & guidelines.....11

4.0 Choosing the right deployment strategy for your school district.....13

5.0 How to choose a provider.....17

6.0 Frequently asked questions.....19

7.0 About Smoothwall Filter.....20

8.0 Contact us.....21

1.0 About this document

The goal of this white 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 technology leaders are choosing to follow a hybrid model where on-premise and cloud computing coexist.

Essential reading for: Technology directors and other technology personnel in K-12 school districts. Also, Superintendents and other school leadership wanting a more practical understanding of their IT environments as it relates to digital safety.

About Smoothwall

Smoothwall is a leading web filtering and digital monitoring developer. Since 2001, Smoothwall solutions have protected millions of students worldwide.

We pioneered the development of real-time, content aware web filtering and have since launched further monitoring and digital safety solutions to protect users in today's world.

Proactively developing and improving our products based on the needs and requirements of schools is what we do best and is what makes us a leading safeguarding provider in education.

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.

smoothwall®

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. The change has impacted schools so much so that many schools have chosen to abandon their on-premise environments altogether. A recent survey of school technology leaders by the Consortium for school Networking found that 88% of districts now use cloud-based educational software systems¹.

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

Major technology vendors emphasize 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 centers versus moving to the cloud.

With restricted budgets and often complex requirements, keeping up with changing technology can be challenging for schools. It's essential for schools to have current systems to better protect students in their care.

1. CoSN's 2018-2019 Annual Infrastructure Survey Report. The School Superintendents Association, MDR, Forecast5 Analytics, 2018, CoSN's 2018-2019 Annual Infrastructure Survey Report, www.cosn.org/sites/default/files/CoSNs%202018%202019%20Annual%20Infrastructure%20Survey%20Report%20final_0.pdf.





With restricted budgets and often complex requirements, keeping up with changing technology can be challenging for school districts. It's essential for districts to have current systems to better protect students in their care.



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 centers 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 do not offer 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 district'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 programs. Additionally, students tethering devices to hotspots are fully filtered.
- **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 students and staff fast access on any device. Simplified user authentication also makes for a more streamlined process.
- **Fast deployment** - Removes the need for the installation of complicated hardware or staff training, allows the system to get on-site and work without a lengthy configuration.
- **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 district's network to expand or contract quickly, ensuring optimization for current usage.
- **Always latest edition** - Cloud filtering will always run the latest version without having to run updates on servers.
- **No bottlenecks avoiding choke points** - Cloud filtering happens at device level, activity is distributed across all devices.
- **Security** - Data in the cloud is encrypted and held on remote, physically secure sites.
- **Data backup** - Cloud services are much more likely to have easy recovery of any lost data or outage.
- **Simplified content filtering** - Some solutions allow real-time, content aware filtering without the complexity of man-in-the-middle (MitM) decryption, certificates, or exceptions.
- **Lower energy costs** - Without the need for high power servers to run 24/7, lower energy costs are expected.

2.2 Traditional on-premise

Most school technology leaders are familiar with installing their web filter on their district's own computers and servers. In many cases, on-premise systems are easier to modify. The ability to customize to specific needs is important for an organization with unique needs.

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 organization is capable of safeguarding its most sensitive information which can be a frequent target of cybercriminals.

Schools with Bring Your Own Device (BYOD) programs can often face issues when implementing a filtering policy. To best address any BYOD trouble, an on-premise filter delivers the best option for creating effective BYOD functionality.

In general, on-premise web filtering may be better suited for larger schools and districts with higher budgets; those that have a desire to customize system operations; and those with existing infrastructure to host, maintain, and protect data.

The benefits of on-premise filtering:

- **Budgets for improvement** - Your organization may have separate budgets for significant infrastructure changes. A major on-premise filtering purchase might qualify for assistance through government grant programs.
- **Upfront cost/subscription** - With most of the cost arising from the initial outlay, institutions that use systems for long periods of time may calculate less overall spending than a regular subscription service.
- **Data security** - Data security remains in the hands of your school. This can give peace of mind provided there is supplemental protection in place.
- **Customization** - Deployment may take longer with on-premise systems, but it allows for more customization to your infrastructure. This can benefit if your school/district has large or complex systems.
- **Existing infrastructure** - Schools and districts are advised to review their current infrastructure and existing contracts carefully to make sure introducing cloud will not result in a duplication of cost.
- **Being ready** - Big changes to infrastructure and systems can add more upheaval in times of other change. It may not be the right time for your school or district to consider a complete systems overhaul.
- **Extra training of staff** - Existing technology personnel will need to understand the system changes for moving over to cloud. This will involve extra training and may initially require additional support.
- **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 district may want to retain total control over its filtering set-up.
- **Consolidation** - Filter appliances might double up as firewalls, making at least part of the purchase eligible for E-RATE funds. Additionally, consolidating both services can maintain 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 an attempted bypass.

2.3 Hybrid deployment

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

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

A hybrid deployment usually retains a less powerful hardware appliance on-site and is combined with client deployment for a portion of student systems. These deployments may start as heavily skewed towards the existing on-premise solution where an organization 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 or districts that may be concerned about any of the following:

- **Managed devices off-site** - There is a growing need for schools and districts to filter managed school-owned devices off-site. If that applies to your school, 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 planning to roll out programs such as a 1:1 initiative, which will involve adding more devices over time. Hybrid can be ideal for meeting flexible and changing requirements.
- **Bring Your Own Device (BYOD)** - Some schools and districts require the benefits of cloud but also want the most effective filtering for BYOD. Hybrid allows you to achieve both.
- **Load distribution** - As internet traffic increases, the need for powerful filter hardware can arise. With bandwidth costs decreasing, 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, the need for additional authentication methods can be removed, particularly for newer devices such as Chromebooks, improving the accuracy of filtering and logging, and ultimately improving digital safety outcomes.



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



3.0 CIPA requirements & guidelines

For school districts that require government e-rate funding, it is a good idea to revisit the Children's Internet Protection (CIPA) requirements and guidelines to ensure you are compliant.

CIPA imposes certain requirements on schools that receive discounts for Internet access or internal connections through the e-rate program – a program that makes certain communications services and products more affordable for eligible schools.

Schools subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are:

- Obscene
- Child pornography
- Harmful to minors (for computers that are accessed by minors)

Schools subject to CIPA have two additional certification requirements:

- Their Internet safety policies must include monitoring the online activities of minors
- They must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Internet Safety Policy

Schools subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools subject to CIPA may not receive the discounts offered by the e-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. Schools must certify they are in compliance with CIPA before they can receive e-rate funding.

- CIPA does not apply to schools receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters internet access.

The school must enforce the operation of the technology protection measure during the use of school-owned computers with Internet access, although an administrator or other authorized person may disable the filtering measure during use by an adult to enable access for educational or other lawful purpose. For example, a school that uses web filtering software can set up a process for disabling that software upon request of an adult user through use of a sign-in page where an adult user can affirm that he or she intends to use the computer for educational or other lawful purposes.

CIPA uses the federal criminal definitions for obscenity and child pornography. The term "harmful to minors" is defined as "any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors."

Decisions about what matter is inappropriate for minors are made by the local community. E-rate Program rules specify that "[a] determination regarding matter inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination."

Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. For private schools, public notice means notice to their appropriate constituent group.

Additional meetings are not necessary – even if the policy is amended – unless those meetings are required by state or local rules or the policy itself.




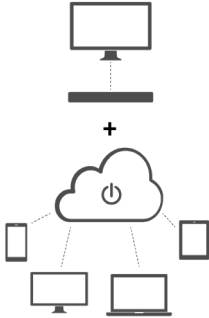
4.0 Choosing the right deployment strategy for your school district

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.

Although cloud environments are becoming increasingly popular, on-premise web filtering is unlikely to disappear altogether. Many on-premise environments find having a physical appliance more reliable to manage.

4.1 Where is your school district on your filtering roadmap?

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

Current needs	Possible solution	Solution detail
<p>Your school district has heavily invested in an on-premise solution.</p> <p>You have the staff available to maintain and manage this equipment.</p> <p>You want to have full control over your system and data, you don't mind completing updates on your devices, and do not want to overhaul a system that is reliable with the opportunity to manually improve.</p>	<p>Traditional: On-premise</p> 	<p>Updating your on-premise solution may be the right place for you now.</p> <p>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.</p>
<p>Your school district has quality on-premise equipment but is noticing gaps in some of the filtering requirements you need.</p> <p>Your school district has available staff to maintain the equipment but need to find a solution that will cover the filtering gaps.</p> <p>Your school district has a limited budget but is in need of a solution that can cover your school district's changing environment.</p>	<p>Hybrid: Traditional on-premise combined with cloud add-on</p> 	<p>A hybrid solution can allow your school district to keep its functioning on-premise solution but implement an add-on using a cloud solution on top.</p> <p>This can be an easy fix without a big overhaul of the existing solution. Your school district can gradually progress over to the cloud, giving you time to plan for meeting all of your complex requirements exclusively through the cloud.</p> <p>By using a combination of on-premise and the cloud, you will be able to achieve greater cost efficiencies, simplify solution management, and improve your content filter's overall performance.</p>

Current needs

You want to overhaul your school district's filtering system and bring your district fully into the modern IT environment.

You don't want to have a huge capital expenditure outlay and are looking for a solution that reduces expenses with a subscription-based cost.

You want to have flexibility in your offering to fulfill your changing device-specific requirements, fluctuating enrollment numbers, and support an ever-increasing number of 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 other technical demands.

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 an overwhelming amount of managed devices and no BYOD program.

Possible solution

Cloud: Advanced all in the cloud filtering

**Solution detail**

Installing a fully cloud-based solution will enable you to create a filtering infrastructure designed to accommodate future technical changes.

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. A cloud solution will enable you to keep your solution flexible so that you can scale up or change flexibly over time.

Data in the cloud is normally encrypted and stored in a remote and physically secured site. This is likely more secure than a school district can achieve.

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, activity is distributed across every device, avoiding bottlenecks.



4.2 Case scenarios

Case scenario A

School District of 10,000 students

3,000 PCs, 7,000 iPads

School District A would like to simplify filtering on their wireless devices. They find the complexity of 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 technical support readily available 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. Since there are no serious issues when 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.

Case scenario B

School District of 1,000 students

700 PCs

School District B have made large investments in their on-premise filtering equipment. They are currently reasonably happy with their filtering set-up but are concerned that if other districts in their state are moving over to the cloud, they will soon be unable to meet the level of filtering required. They have the staff to keep up basic 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 that are able to maintain an on-premise solution, the school district will be able to keep up-to-date by simply updating their appliance-based solution. Although they will not be able to enjoy 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.

Case scenario C

Educational Service Center of 17,000 students

5,000 PCs, about to introduce 12,000 Chromebooks with more to be added over following years

Educational Service Center 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 also are looking for flexibility and scalability as they want to trial with their 3,000 high schoolers first before rolling it down at the middle school level.

Solution: Hybrid or cloud

The ESC is looking to make significant changes to their IT structure. With the plan to roll out 3,000 managed devices to middle school students, and then to increase this across the rest of the region over time, cloud filtering would provide the best solution. It will enable the ESC to achieve fast deployment and easy scalability as the number of devices increase.

Case scenario D

School District of 5,000 students

800 PCs, 1,000 Macs, 2,000 Chromebooks

School District D has a smaller technology department who are struggling with the time needed to maintain an up to date on-premise filter while having to manage the rest of the district's technology needs. They also have large 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 2,000 Chromebooks and need easy deployment and flexibility of on and off-site filtering.

Solution: Cloud

Cloud reporting will reduce the need for staff management and maintenance. The most updated version of filtering will always be automatically be available without needing a 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 provider

When choosing a provider, it is important to choose a solution that covers all the requirements as part of CIPA. Looking for a vendor that is established and a specialist in solutions for education and the public sector 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 the necessary filtering requirements. Having room for customization is also key when selecting a provider.

5.1 Checklist of functionality

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 categorizes content by analyzing 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 educators.
Powerful real-time reporting	Look for a provider that offers timely reporting. A provider should empower school districts to take a proactive approach and intervene in concerning behavior before it further develops.
On/off-site protection	If your school district has any managed student devices, it's necessary to make sure 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 and provide evidence-based reporting to administrators.
Authentication	Look for a simple authentication process that makes access smoother and makes it easier to track all users.
Social media controls	Check that the solution gives you options around social media including read-only access.
Anti-malware	Ensure the solution covers protection against malware and ransomware threats.

Data security Ensure that any vendor understands any specific requirements around school data.

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 prioritize the ones you do.

Anonymous proxy-blocking Look for a simple authentication process and allows to easily track all users.

Age appropriate Look for filtering providers that use a wide variety of directories (e.g. Microsoft AD, Google Directory) and allow filtering to be set appropriately at group and/or 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 analyze 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 provider that can offer a solution that best suits you. A good vendor will be able to look at your needs and provide a tailored solution to meet all your requirements.

Deployment Check that the speed of deployment and the resources you will need on-site match up. Many cloud solutions can have a faster set-up than on-premise. Less configuration and equipment on-site makes cloud filtering deployment a speedy process.

Scalability Check that your solution will easily adjust depending on your school district's ever-changing network needs. Adaptability is key for a long-term solution.

Provider reviews Look for providers that can show you an established history in providing filtering for US education. New providers may offer services that are "too good to be true" as they do not fully address the needs and challenges of filtering in education and may not be able to deliver what they are promising.

Support A quality 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 school districts look to introduce 1:1 initiatives is the protection of the devices when they are away from the school's supervision. They want the district to offer peace of mind in having the risks covered in and outside of school.

Will my data be secure in the cloud?

With school districts being vulnerable targets for sensitive data breaches, data security is critical. Most providers using the cloud are likely to suggest that using the cloud is more secure than on-site. Smoothwall uses Microsoft Azure – some of the most certified and secure data centers, 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 costs. This gives districts the flexibility to change the set-up over time.

Is on-premise more customizable?

In complex or large systems, on-premise or hybrid solutions can offer institutions more detailed customization 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 changing needs. Many providers operate in tiers of user quantity with the possibility to change tier over time.

Will cloud filtering make my old equipment redundant?

Not necessarily. If your school district 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 full and successful 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 categorization and assess the content of pages - not just the URL. Leading providers like Smoothwall have intelligent, rules-based mechanisms that allow sites to be more accurately classified and filtered upon, without unnecessary access restrictions.

Have a question that's not answered here?

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

Tel: 800.959.3760

Email: inquiries@smoothwall.com

Web: us.smoothwall.com/contact-us

7.0 About Smoothwall Filter

At Smoothwall we know that the needs of school districts are changing. We know that the internet is now an integral part of education and that the need for flexibility and mobility of devices is increasing. Changing requirements mean school districts may need a variety of solutions.

We have added Smoothwall Cloud Filter and Hybrid deployment in addition to our on-premise offering, to meet these needs and enable you to take your web filtering to the next level. Your school district is no longer restricted to only filtering on-site or tied to the speed in which your filtering can be deployed.

The added benefits that Cloud Filter offers are:

- Filtering devices both on and off-site.
- Flexibility and easy scalability so that your needs can be met overtime.
- Simpler configuration without the need for man-in-the middle, certificates, or exceptions to use real-time content analysis.
- 100% time-line reporting meaning that a full, evidence-based picture can be created around incidents.
- Side-stepping choke and throughput issues.
- Safe and fast internet access.
- Faster installation process and more robust user authentication.
- Security of data encrypted within remote and physically secured sites.

Other key elements offered by Smoothwall Filter include:

Real-time dynamic content analysis: Smoothwall provides filtering and reporting that analyses and categorizes web content in real-time. Schools can be better protected than they would with URL blocklists that frequently 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 that include read-only settings and inappropriate content removal from school sites.

Gateway anti-malware (on-premise only): Whether a user opens something by accident or deliberately tries to access something containing malware, Smoothwall's anti-malware will protect your school district from malware and ransomware threats.

Layer 7 application control (on-premise & hybrid only): You can choose which applications you want to prioritize on-site and remove applications you don't want on your network.

Easy management (on-premise): Easy bandwidth management and allocation means you can minimize bandwidth use when the need for media usage or file sharing increases.

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

Next generation firewall (on-premise & hybrid only): Protect yourself from all web and non-web borne threats by monitoring all incoming and outgoing traffic.



Contact us

If you would like to learn more about any aspect of your web filtering and its deployment, our specialist team is ready to help.

Please contact us.

Tel: 800.959.3769

Email: inquiries@smoothwall.com

Web: us.smoothwall.com/contact-us

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 quote.

us.smoothwall.com/contact-us

Further reading

You may also be interested in:

Digital Safeguarding - Reducing violence in schools with digital monitoring

Our free guide is designed to empower district administrators with the essential knowledge needed to make informed decisions on monitoring technology for schools.

Available at <https://us.smoothwall.com/digital-monitoring/>



Smoothwall

1435 West Morehead Street
Suite 125
Charlotte, NC 28208

Tel: 800.959.3760

Email: Inquiries@smoothwall.com

us.smoothwall.com

 [SmoothwallUS](#)

 [SmoothwallUS](#)

 [Smoothwall-Inc](#)

 [SmoothwallTV](#)

© Smoothwall Inc. This document is the copyright work of Smoothwall Inc. and may not be reproduced (in whole or in part, in any form or by any means whatever) without its prior written permission. The copyright notices and trademarks on this document may not be removed or amended without the prior written consent of Smoothwall Inc.

smoothwall®