Smoothwall for Education

Whitepaper

Digital Safety

How to Achieve **Digital Safety Excellence** Across a Multi-Academy Trust

A best practice guide for Trust leaders and DSLs.

Provides the practical steps needed to raise standards across your organisation in the most time and cost-efficient way.

smoothwall®

smoothwall.com

Whitepaper

Contents

About This Document

Keeping students safe online goes beyond minimal compliance and beyond a tick in a box approach. Online dangers are not going away and those MATs with a child centred approach to safeguarding understand this, and take great care to ensure students and staff are protected at every touch-point.

Creating a standardised model of online safety excellence is not for the elite few. It is becoming a mainstream intention in MATs across the UK. The benefits are far reaching:

- Student safety
- Network safety
- Ofsted compliance
- Reassurance to parents
- Reputation and reassurance to support new school acquisition
- Improved learning and academic attainment
- Improved student behaviour
- Efficient, standardised practice across the Trust.

This guide has been prepared by Smoothwall's digital safety experts to help MAT leaders and DSLs understand what excellence looks like. It offers the practical steps needed to raise standards across your organisation in the most time and cost-efficient way.

It is designed to help your MAT become a beacon of excellence in online safety.

Essential reading for:

CEOs, Headteachers, DSLs and anyone responsible for safeguarding across a Multi-Academy Trust.

Contact us

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®

1.0 A Regulations Refresh

With the online space constantly evolving, Ofsted and statutory guidance are continually being updated. It can be a challenge to keep up. Below is a handy refresh of the key points.

KCSIE 2019 Statutory Guidance[1]

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[2]

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[3]

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.

Ofsted summary value evaluations[4]

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.

The UK Safer Internet Centre[5]

The UK Safer Internet Centre provides helpful advice in the way effective filtering and monitoring should look. KCSIE 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".

Keeping children safe online goes beyond minimal compliance. It should never be considered a simple ‘tick in a box’.

2.0 The Unique Factors of a Multi-Academy Trust

As a MATs you have a multi-layer accountability for governance across your Trust.

This can be a complicated business, especially when dealing with different schools, across different geographical spaces and at different stages of digital safety maturity.

This does offer some unique benefits however. A group of interconnected academies is a platform to share best practice. It also allows centralised procurement which saves time and money, and a centralised support to maintain operational standards.

Crucial to leveraging these benefits is flexibility and variation in your digital safety model. Using a technology partner whose solutions, delivery and purchasing models are not rigid but are instead uniquely geared to maintaining excellence while accommodating grassroot variables in your MAT is key.

"The strength of MATs in building teams that have finance, HR, IT and site management expertise means that more teachers and leaders can focus on what they do best; great teaching."

Department for Education, 2016.

3.0 Digital Safety - The Excellence Model

3.1 Why excellence matters

We're not in Kansas anymore. As the internet and technology within schools continue to evolve at a rapid pace the need to adopt high and centralised standards in digital safety become paramount.

Excellence in online safety is no longer an option.

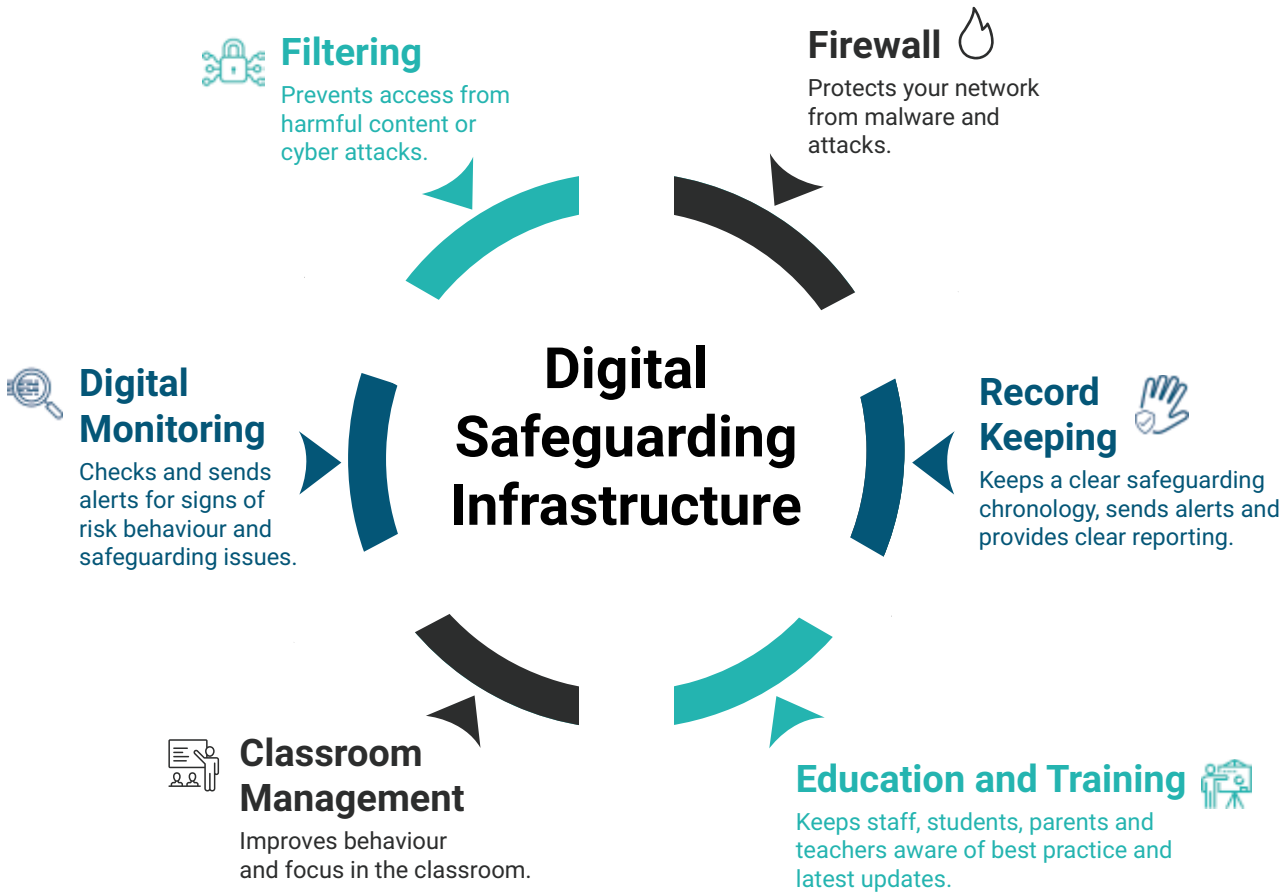
The benefits are far reaching:

- No more interruptions to lessons caused by lack of bandwidth.
- Online learning resources are freed up. Updates to safeguarding records are timely and access is easy.
- Time needed by the DSL to trawl through online logs is vastly reduced.
- Additional DSL stress and worry over missing a safeguarding concern is eliminated.
- Ability to track user groups across schools.
- Interoperability between different safety technologies.
- No more damage to networks caused by software or document downloads.
- Protection against data breaches and cyber attacks.
- Cost efficient and reliable technology.
- Ability to identify students who may be at risk including self-harm, suicide, bullying, radicalisation, grooming, abuse, drugs, gang membership, exam stress and others.
- Improved learning and more dynamic classrooms.
- Education and learning about online safety for the whole school community – everyone becomes an expert.

3.2 The excellence model

The diagram below illustrates a six pronged approach to student, teacher and network safety. It is a centralised online safety infrastructure that transcends all areas of your MAT including every digital touch-point.

Every MAT is unique in its set-up and there is no 'one type fits all'. Some Trusts will be ready for a centralised online safety infrastructure, whereas others will still retain autonomy at academy level.



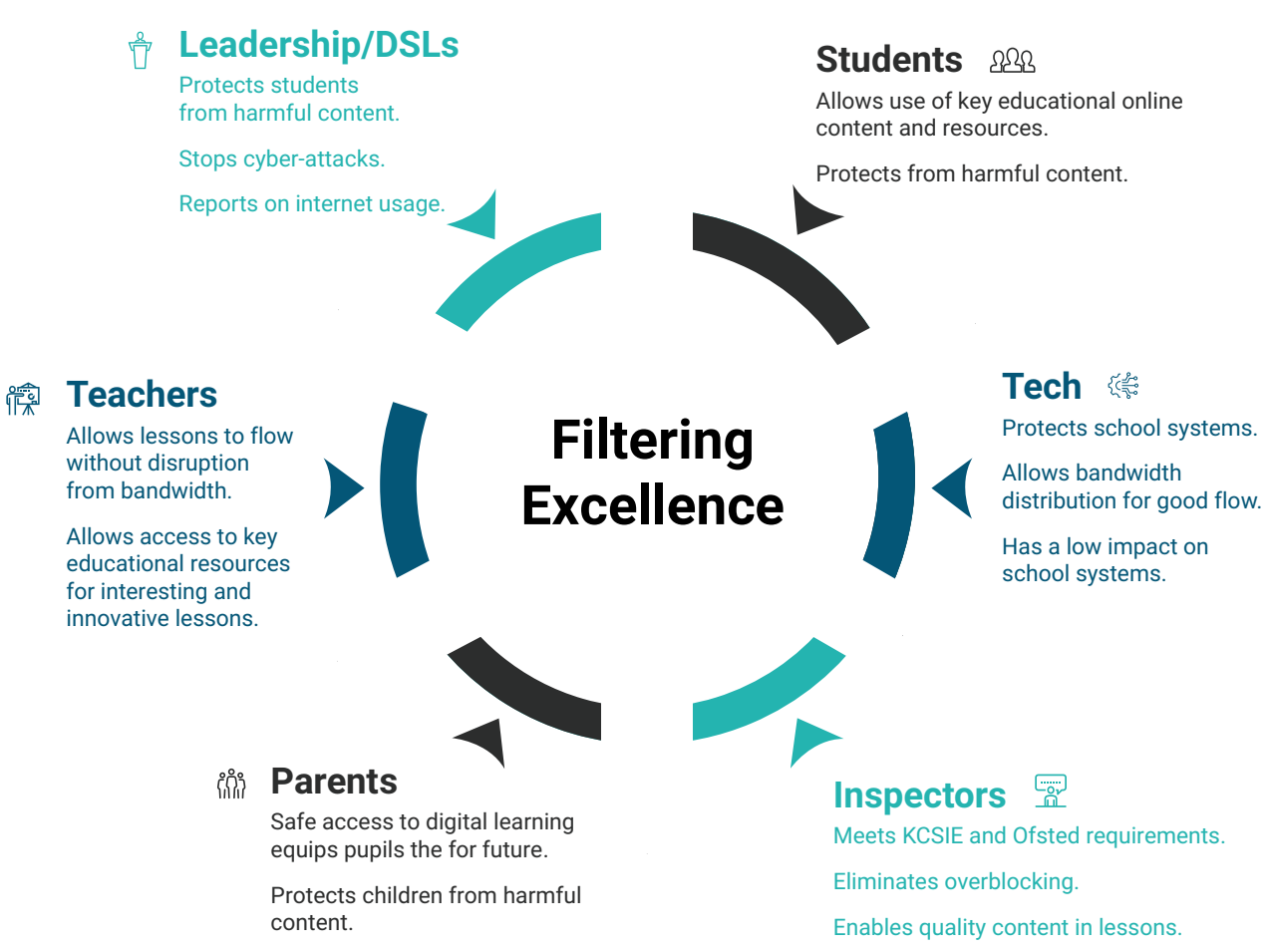
Regardless of where you are on your excellence journey understanding basic versus advanced capability in each area will help with incremental improvements.

Explore the differences between basic and advanced components of an online safety infrastructure on the following pages.

3.3 Filtering

Filtering helps your MAT community to keep users safe online and is part of safeguarding statutory guidance. It blocks illegal and inappropriate content and keeps your systems protected.

Best practice is to find a system that will work within different user groups and access levels. The diagram below shows the far reaching benefits of good filtering.



Basic vs advanced filtering capability

Basic filtering	Advanced filtering
Limited access levels Has the same level of access for all users. This could lead to issues in safeguarding and data control.	**Varied access levels** Allows a multi-layer of access. Different staff members have different responsibility access.
Anonymous users Has a lack of user identification especially BYOD users.	**User identification** Provides 360 identification view of users, all activity on any device combined.
Bandwidth limitation Does not permit bandwidth variation across a MAT or Academy.	**Real-time bandwidth allocation** Has varied controls across a MAT or Academy depending on requirements.
Blocklist filtering Uses blocklists which can lead to inappropriate content access and over-blocking.	**Dynamic filtering** Provides content analysis in real-time which avoids over-blocking and inappropriate access.
Circumvention Can be circumvented by capable students via VPNs and anonymous proxy servers.	**No circumvention** Cannot be circumvented by VPNs and anonymous proxy servers.
Device coverage Has limited device coverage which risks online safety and systems.	**Device coverage** Covers all device requirements including iOS and tablets.
User settings Doesn't allow the variable settings needed for different user groups, age ranges and settings.	**Variable settings/reports** Offers varied access for different ages or user groups.
Social media Has a single option to block or unblock social media.	**Social media controls** Has multiple options for social media control e.g. by age group, by type of access as well as read-only mode.

Continued.

Basic filtering	Advanced filtering
Deployment May only give one deployment option. MATs often need solutions with varied deployment.	**Deployment** Different deployment options include on-premise, cloud or hybrid which allows the right set-up for your MAT.
Firewall threat protection Is limited in protecting against threats such as ransomware, malicious content and cyber-attacks.	**Firewall protection** Has advanced protection with intrusion detection and prevention reports on any malicious attacks.

Illustrative case scenarios

The following scenarios show what basic versus advanced filtering means in practice.

Basic filtering in a MAT

Example 1
Some devices in the Trust are not covered leaving online systems exposed.

Example 2
A DSL has the same access to filtering reports as an IT tech officer risking safeguarding.

Example 3
Online infrastructure is varied across the MAT leading to excessive costs.

Example 4
No overview for leadership to identify trends and solve issues across trust.

Advanced filtering in a MAT

Example 1
All Trust devices are protected by filtering to keep systems safe.

Example 2
Access is set-up with responsibility levels so that correct and secure access is given.

Example 3
Standardisation maximises cost savings and boosts protection.

Example 4
Trends of online behaviour are identified. Issues can be addressed across the MAT.

3.4 Digital monitoring

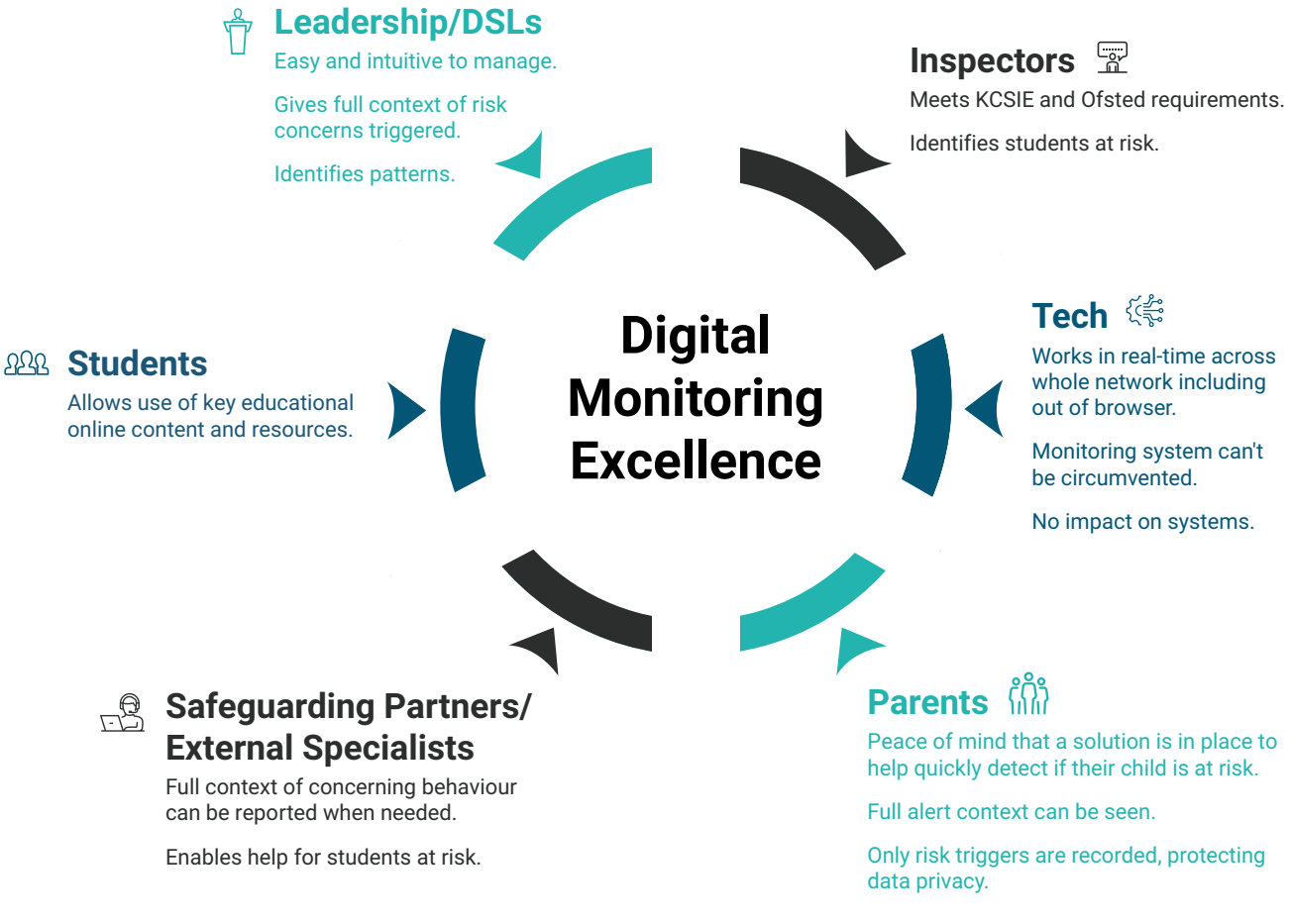
Monitoring is an important means of early identification for children who may be at risk. The earlier the intervention, the better the outcomes. It is part of school statutory safeguarding guidance for this reason.

By identifying issues at an early stage, Trusts can tackle a concern before it escalates into something more significant.

The types of issues digital monitoring can help safeguard against include: bullying, mental health issues, substance abuse, gang membership, exploitation and abuse, self-harm, radicalisation and others. It also enables more students to reach their maximum potential and could reduce student absence.

Monitoring solutions vary in the time and supervision they require from you to function properly. For MATs with a high student population, having an external team of safety experts monitoring your alerts may be more appropriate. This real-time service can avoid incidents being missed by busy staff and reduce the time needed to manage false positives.

For some MATs who have available staff and complicated customisation needs, a self-service option may work better. Looking for a provider that offers all options will ensure you find the right solution for your organisation.



Basic vs. advanced digital monitoring capability

Basic monitoring	Advanced monitoring
Management Systems reliant on logs wastes DSLs time searching for risk concerns.	**Management** A managed service involves safety specialists checking risk-triggers and alerting DSL.
Delayed function Many systems do not report alerts in real-time. An urgent concern may be missed.	**Real-time** Works in real-time. Urgent risks can be seen and acted on straight away.
No pre-grading No pre-grading makes it difficult to know which alerts need to be followed up and can result in more false positives.	**Pre-grading** The seriousness of an alert can be judged by intelligent pre-grading and can filter out many false positives saving valuable time.
Basic reporting Limited reporting showing only a web address of an alert makes it difficult to follow up.	**Full context reporting** Full context of a capture is shown with detailed information or a screenshot.
Circumvention Monitoring could be circumvented.	**Circumvention** Cannot be defied by VPNs or anonymous proxy servers.
In browser Misses vital activity such as online web-chats and emails.	**Switch on to switch off** Captures all risk activity in or out of browser from log-on to log-off.

Illustrative case scenarios

The following scenarios show what basic versus advanced monitoring means in practice.

Basic digital monitoring

Example 1
Needing to trawl through hundreds of logs makes it easier for the DSL to miss online incidents.

Example 2
Physical monitoring puts additional strain on teachers.

Example 3
Trust leadership are limited to occasional reports created by schools.

Example 4
Students out-of-browser activity is not monitored. Safeguarding concerns can be missed.

Advanced digital monitoring

Example 1
Managed monitoring alerts DSL of online incidents in real-time. False positives are removed.

Example 2
Teachers can focus on teaching knowing monitoring will identify risk-concerns.

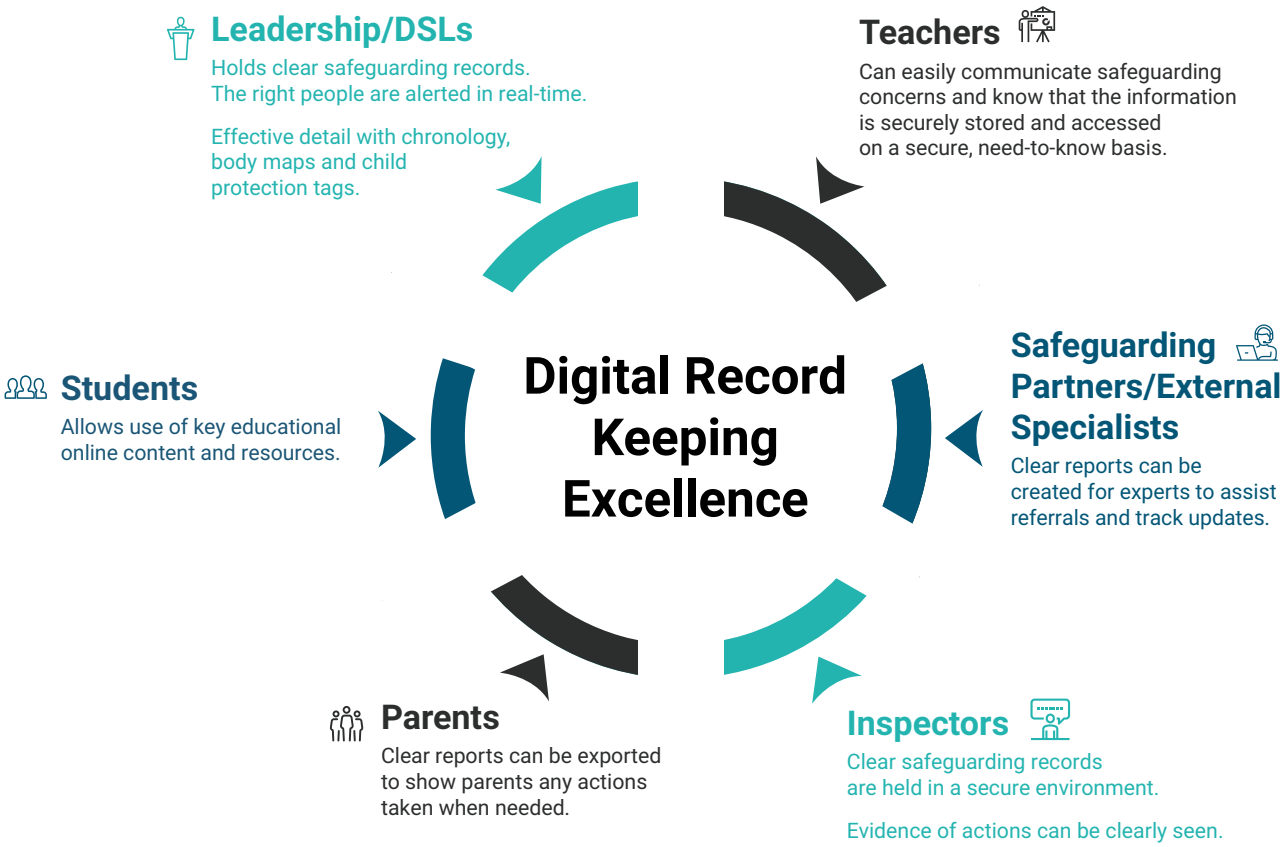
Example 3
Trust leadership can gain access, identify trends and check for contextual safeguarding issues.

Example 4
Risk concerns out of browser such as webchats, emails, word docs etc can be picked up.

3.5 Digital safeguard record management

The ability to access safeguarding records in an instant can be really helpful for MAT leadership. You can check on cases and see how risk groups within the MAT are being tracked. An advanced solution enables leaders to tag certain pupil groups such as 'child in need' and be able to see all relevant information for that specific student group across all their academies.

A digital solution for safeguarding records is a living digital document that can be updated easily and provides alerts and access to relevant parties efficiently with tiered, secure access.



Basic vs. advanced record management

Basic record management	Advanced record management
Updating records Physical record keeping makes it difficult for files to be updated easily and key information could be missed.	**Updating records** Staff members can add concerns to records straight away. They can alert the required members of staff in real-time.
Creating reports Physical records are more difficult to share and need more time to produce.	**Creating reports** Clear reports can be created. Necessary information for relevant parties can be shared securely.
Tracking referrals Key concerns or referrals that need to be made can be forgotten when the system does not have clear oversight of follow-up.	**Tracking referrals** Concerns are digitally tracked, reminders can be sent to staff and a clear oversight of follow up is available.
Accessing records Physically held records can limit access. Storing a version on a shared area can mean data is not secure.	**Accessing records** Excellent software can ensure both secure access and that the right people can access the records on any device, anywhere.
Student group tracking Limited record keeping may mean that it is difficult to track specific areas such as 'CP Plans' and 'Child in need'.	**Strong group tracking** Tagging students in particular areas such as 'CP plans' and 'child in need' allows you to track specific student groups across the Trust.
Information gathering May lack detail in records from other systems such as online incidents that have taken place and body maps may not be able to link without having to interpret manually.	**Full information gathering** A full chronology of a student can be seen instantly. Online incidents can be directly linked without having to be recorded again. Body maps can be created to look for emerging patterns.

Illustrative case scenarios

The following scenarios show what basic versus advanced record keeping means in practice.

Basic record management in a MAT

Example 1
A lack of overview can lead to issues not being addressed quickly in schools.

Example 2
Urgent access to records cannot be made to the Trust leader when not on site.

Example 3
Reporting on specific student groups is limited and relies on a paper chain.

Example 4
A busy DSL could miss follow up on a safeguarding concern as there is no clear process to check follow up.

Advanced record management in a MAT

Example 1
Leadership has full overview of safeguarding-records. Acadamies needing support can be identified.

Example 2
If a serious incident occurs, Trust leadership can securely access a student record immediately.

Example 3
Student group tags enable leaders to analyse specific groups easily.

Example 4
A busy DSL can set-up reminders to ensure safeguarding issues are acted on correctly.

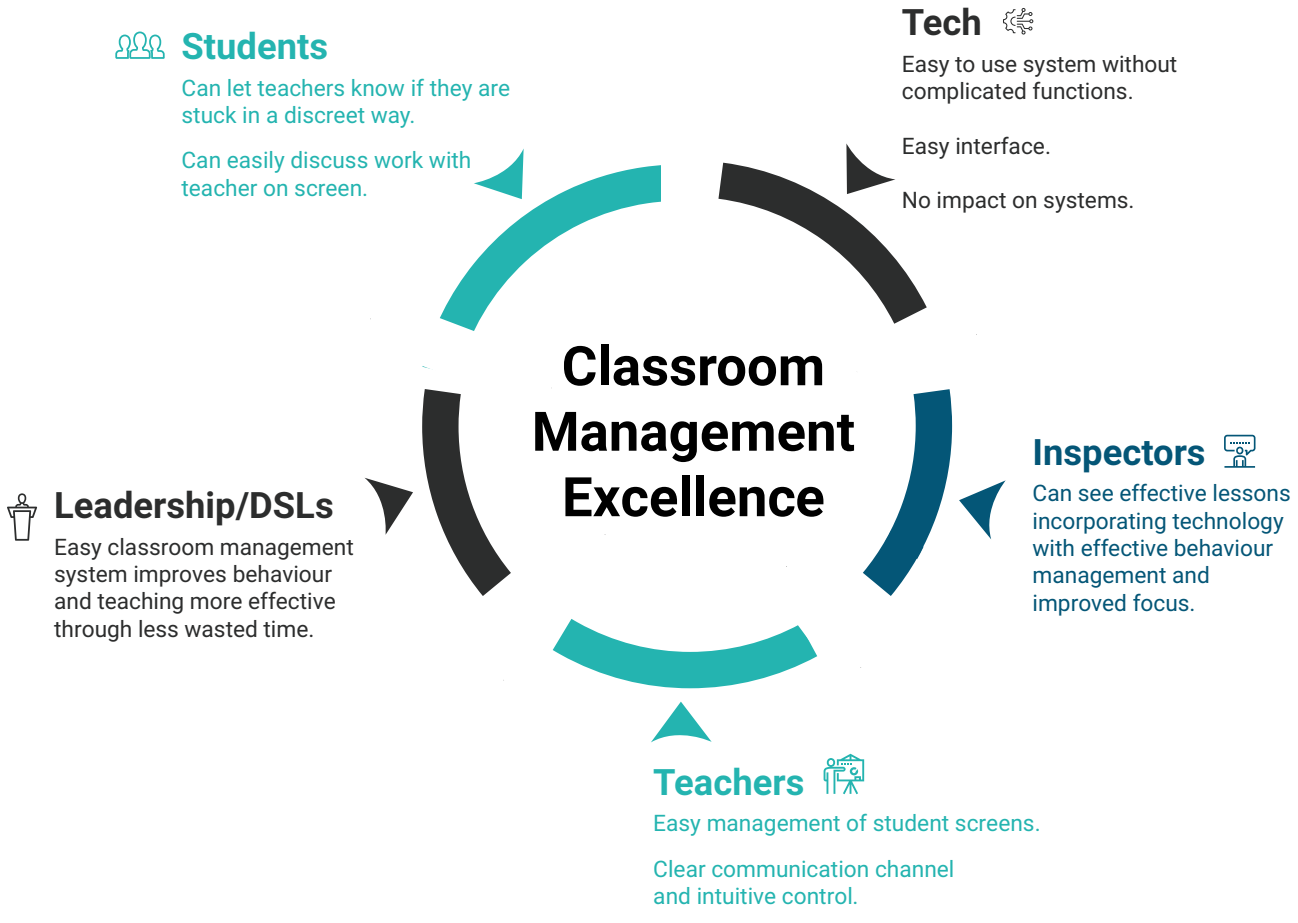
3.6 Classroom management

No matter how focussed and motivated, a classroom of students all simultaneously working on computers can be a challenge for even the most competent of teachers. Making sure that every individual is on task and concentrating can be difficult.

An effective classroom management system enables teachers to maintain a dynamic, focussed, and productive learning environment at all times. They can instantly disable screen access, as a group or individually; they can see if anyone has jumped off task, and can quickly see and address any misbehaviours, without disrupting anyone else.

Classroom management systems are only effective when they are intuitive. Teachers prefer systems that are easy to use and do not, in any way, detract from the role of teaching.

The diagram below shows the far reaching benefits of an effective classroom management solution.



Basic vs advanced classroom management

Basic classroom management	Advanced classroom management
Operation May be complicated to set up and use. Ability to track all students at once is limited.	**Operation** Is intuitive and easy to use. Lessons can run smoothly without becoming stuck on operational issues.
Distractions Could have too many unnecessary features that make it complex to use.	**Distractions** Straight forward using core tools teachers need to run a lesson effectively without unnecessary distractions.
Individual screen view May only give an overview of screens without being able to drill down to individual screens in detail.	**Individual screen view** Teachers will be able to drill down to a single screen to intervene when needed.
Limited of device control Won't allow staff to limit devices e.g. individual devices in exams or whole class control when needing students to listen.	**Device control** Staff can easily limit device usage. This could be whole class or individual e.g. the teacher can lock all screens to regain attention or individual devices can be limited.
Bandwidth limitation Running software may impact on bandwidth e.g. chromebooks can be limited by RAM space.	**Bandwidth limitation** Peer to peer architecture enables low impact on bandwidth.
All focus limitation Unable to control all students' machines together e.g. can't load a specific URL on all devices at once. This can hold up lessons.	**Full session control** Teachers can load URLs for all and easily set session times without needing to involve IT. Easy intervention can be made.
Limited monitoring Monitoring may not occur in real-time and so a teacher could miss a student being off-track.	**Real-time monitoring and evidencing** Allows staff to monitor in real-time and create screenshots of activity when needed.

Illustrative case scenarios

The following scenarios show what basic versus advanced classroom management means in practice.

Basic level classroom management

Example 1
The start of the lesson is held up because the teacher has to help some students who can't load up the right URL.

Example 2
No peer to peer architecture means classroom management slows machines.

Example 3
Teacher misses a pupil who is off task as they have no overview of all the students screens.

Example 4
Teachers avoid using IT in lessons as it causes too many issues.

Advanced level classroom management

Example 1
Teacher spots a student off-task in their full grid view and closes down the pupil's tab to refocus.

Example 2
Teacher takes an evidence screenshot of a student on an inappropriate website and follows up.

Example 3
Teacher sets a time limit on a session so that there is no hold up for the class plenary.

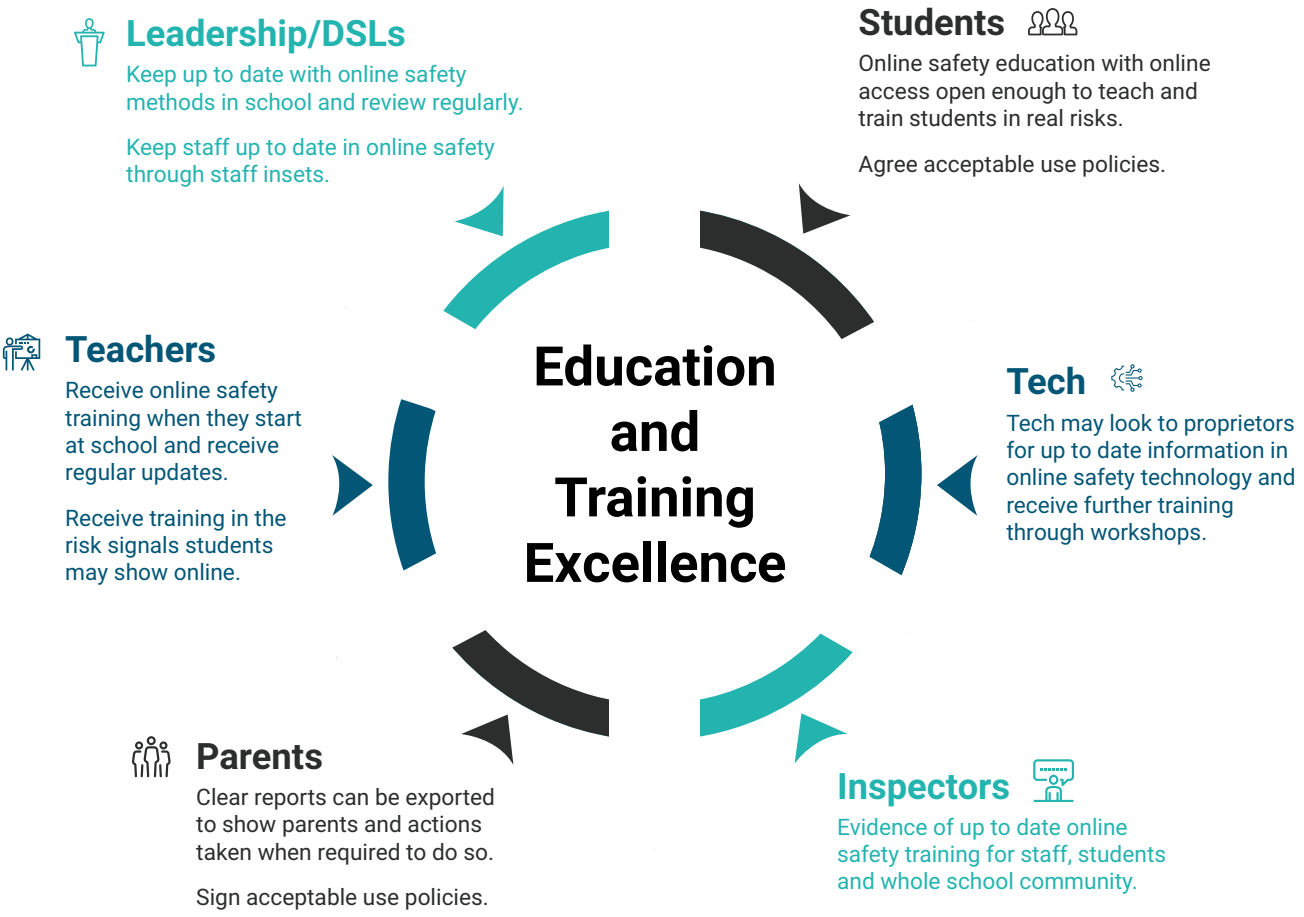
Example 4
Students receive innovative lessons with teachers confident IT will enhance lesson.

3.7 Education and training

Roles and responsibilities

Education and awareness of online dangers is a crucial component in keeping children safe online. Your DSLs are expected to ensure every member of staff is appropriately trained from the moment they arrive at the school.

Education starts with children themselves but it extends to the whole school community, including governors, headteachers, teachers, staff and parents. When everyone understands and follows safe practices, safety online becomes the norm, not the exception.



4.0 Planning For Improvement

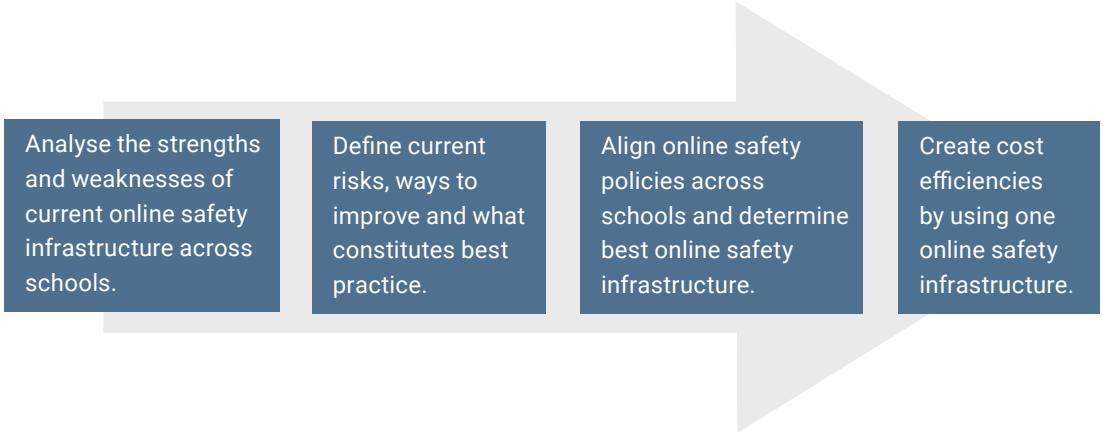
The following are the most common/effective steps used by Smoothwall MAT customers to raise online safety standards.

Step 1: Best practice briefings – Inviting school IT Managers and DSLs to a safety session. The excellence model is explained to them and they are asked to benchmark their current set-up. The table on the next page can help with this. Best practice briefings are a great way to do a skills refresh and underline risk factors that may have been forgotten.

Step 2: Trust-wide analysis - Leaders can use this data to place each academy in order of complexity, and evaluate the positive impact a new standardised online infrastructure can have. They can also carry out a cost savings analysis.

Remember when calculating cost savings to bear in mind the discounts vendors may offer for multiple procurements. Smoothwall's Optimum programme is specifically designed to allow MATs to achieve a centralised excellence model at the lowest possible cost. In some cases, it also allows them to acquire any existing contracts you may be in, but wish to leave.

These steps can be summarised as follows:



4.1 Benchmark planner

School	Element	Questions to consider	Basic	Advanced	Improvement opportunities	Current costs
	Filtering Monitoring Record management Classroom management					
	Filtering Monitoring Record management Classroom management					

4.2 Choosing your technology partner

When your Trust is planning for a centralised infrastructure, or any improvement to its digital safety provision, it's important to consider the following:

Allowing for variation

MATs vary greatly in their organisational structures. For some an individual solution will be all that's needed to raise the bar to excellence. For others a centralised solution across the Trust may be required. An excellent provider will offer different options along with the expertise to help you make the right choice for you.

Consolidation

Acquiring all your solutions from one high quality provider can eliminate technology conflict problems. A single source of support can be a great help if things go wrong. It will also ensure maximum cost savings as previously mentioned.

Training

Check your provider is committed to keeping you up to date with online safety trends. Some offer customer days to share best practice and listen to the needs of school staff.

Data privacy

Academies hold sensitive information about students, staff, parents, and the rest of the Trust community. With reputational responsibility at stake, it is important to protect against the risks of cyber-attacks. It's important to check that you are using the highest rate of data privacy protection possible.

Support

Look for a provider who has proven expertise in UK education and offers UK based support. Solving problems can be more difficult if your vendor doesn't understand your education environment, data privacy laws or struggles with international time delays.

Appendices

Book a demo

Smoothwall are the UK's number one provider in digital safety technology in education and we are the only provider to specialise in digital safety within the MAT environment.

To arrange a no obligation demonstration or speak with an expert we would love to assist. Please contact us.

Contact us on:

Tel: +44 (0)870 1999 500
Email: enquiries@smoothwall.com

smoothwall.com

smoothwall®

Further reading

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

Safeguard Monitoring: How to Prepare Your Case for Funding

A step by step guide for DSLs, Head Teachers, Principals and anyone responsible for ensuring a compliant digital monitoring provision within their School.

Available at: https://smoothwall.com/how-to-create-a-case-for-funding

More papers and articles

To see more papers and articles on digital safeguarding in independent schools, please visit https://smoothwall.com/education/about-you/mat-digital-safety-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.

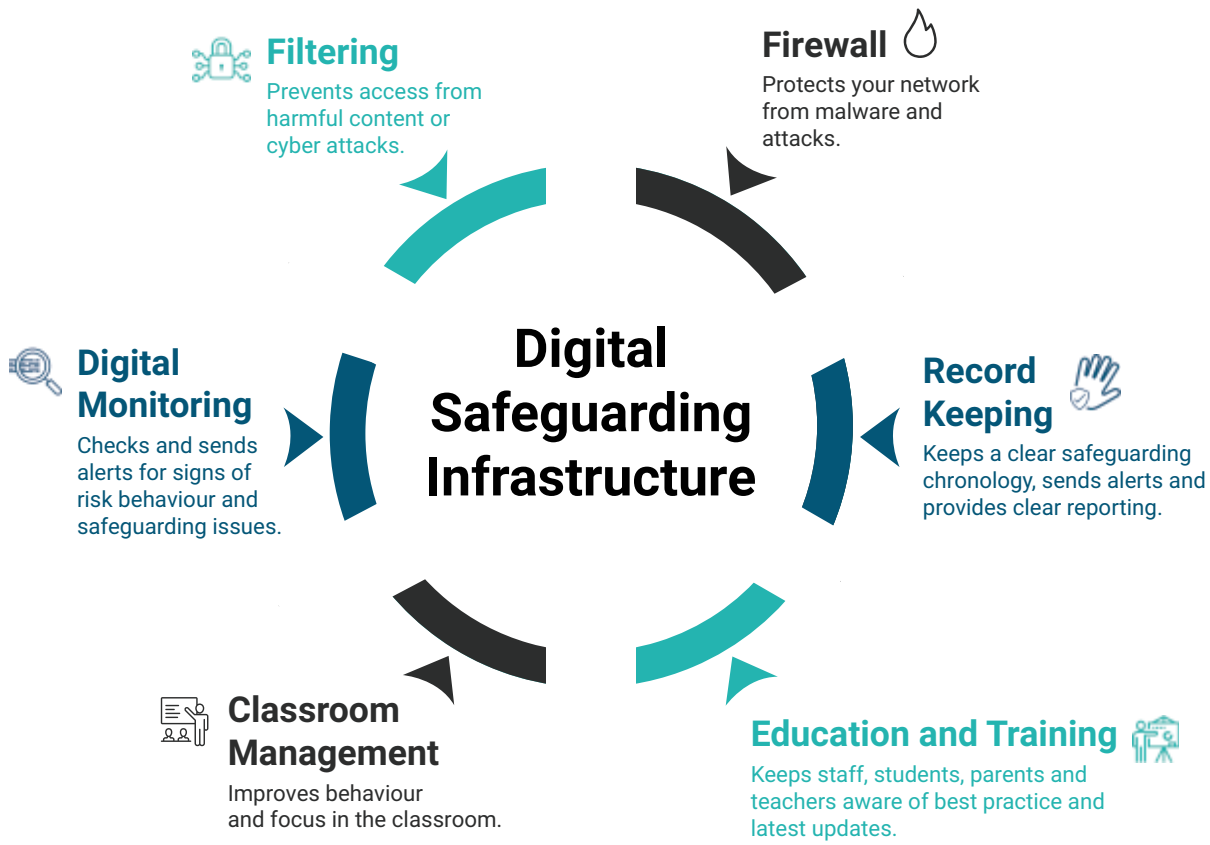
The demands placed on the physical eyes and ears of teachers far exceed their ability to identify all but the most obvious risks, and puts the organisation at odds with both student needs and statutory guidelines.

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. Gov.UK. 2018. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
2. Gov.UK. 2019. https://www.gov.uk/government/publications/prevent-duty-guidance
3. Gov.UK. 2019. https://www.thesun.co.uk/news/8706473/private-school-class-a-drugs-coke-ecstasy/
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®