Active 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 monitoring provision within a school or college.

smoothwall®

smoothwall.com

Contents

Appendices

About this document

This document is a guide to help you create your case for funding for your school's new active monitoring solution.

Written by Smoothwall's Online Safety Experts, it presents the key factors your stakeholders may have together with information and practical guidance on how to address them fully and persuasively.

Essential reading for: Designated Safeguarding Leads, Head Teachers, Principals and anyone responsible for a compliant monitoring provision within a school, college or multi-academy trust.

If you have any questions or require any assistance with your monitoring provision or case for funding please do not hesitate to contact Smoothwall's Online Safety 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 Why Prepare Your Case?

If you have identified a need for improved monitoring within your organisation you may need to present the case to your Head, Principal, Governors or other key stakeholders to secure the necessary funding.

This may feel like a challenge particularly if budgets are tight.

It can also be tempting to turn a blind eye, especially when there are so many other important tasks to attend to. But it's important to remember that cases of online harm to children are often proceeded by warning signs that are not picked up. Added to that is the risk to your school's status if you cannot evidence, when asked, appropriate monitoring measures to Ofsted.

Preparing a strong case to secure the support and funding you need to deploy a compliant monitoring solution is therefore crucial.

There are 7 key factors your stakeholders may want you to evidence before agreeing to fund a new monitoring project:

- Explanations and definitions
- The need for change
- Your areas of non-compliance
- Your statutory obligations
- What monitoring solutions and why?
- Additional benefits
- Possible sources of funding.

This document helps you address each in a clear and compelling way.

It is designed to save you time as well as highlight important factors you may not have previously considered.

2.0 Active Monitoring - Explanations and Definitions

If you are currently using another form of monitoring such as physical monitoring or logging online usage, your school or stakeholders may be unfamiliar with the term ‘active monitoring’.

An explanation of what it is and how it works is an important first step when making your case.

Specifically:

a) What is active monitoring?

b)The difference between active monitoring and filtering

c) How active monitoring creates advanced risk identification?

d)Non-moderated vs human moderated active monitoring

a) What is active monitoring?

Active monitoring (also known as safeguard monitoring or digital monitoring) is a technology system in which digital devices within the school are constantly monitored for signs of risk.

Active monitoring helps you to identify students at risk promptly. Serious risks such as a suicide, grooming, or a gang meeting can all be picked up in real-time if a child has used a device in any way to view content, message someone, look for information, type out their feelings – even if they delete it immediately or never press ‘send’ or ‘enter’.

Active monitoring helps you detect problems and respond to issues you may otherwise be unaware of. It also enables you to help individuals who haven’t previously been shown to be at risk.

For pupils already at risk you can check for escalation and feedback the evidence to relevant bodies.

Active monitoring creates a safety-net for teachers who, in a busy classroom, may be unable to see what is happening online.

b) The difference between monitoring and filtering

Active monitoring is not the same as online filtering.

Where online filtering blocks the content that a child or young person sees on a device, monitoring (depending on the solution you choose) analyses screen views and any keystrokes the user makes into their device to search for risk.

Whether a user types into a browser, an email, a Microsoft document, a social media platform, the monitoring solution will capture the word/s (even if they are immediately deleted, written white on white or never submitted or sent) and create a risk-grade based on it.

Schools are notified of risk alerts in real-time enabling them to act on severe alerts immediately.

c) How active monitoring creates advanced risk identification?

As well as allowing schools to see the online activity of students known to be at risk, active monitoring can also flag students at early risk of harm and who may not be on your school's risk radar. This gives staff the ability to intervene before a concern escalates into a crisis.

Active monitoring can record and alert against predefined words and phrases that are categorised against a theme and level of potential risk, or by building an intelligent profile of a student in context.

The words and phrases that are monitored can be typed or viewed and depending on the solution, can come from any application on the device, not just from the Internet.

d) Non-moderated vs human moderated active monitoring

Non moderated - When a student or staff member types or views something alarming into a digital device, a screen capture is made by the active monitoring system. The system will apply a risk-grade based on the capture. Schools can see risk alerts easily enabling them to act on severe alerts promptly.

Alerts are logged into a console, in real-time, enabling you to see the details as soon as you log in and decide how best to proceed.

By accurately grading risks, schools can decide which alerts need their immediate attention and which can be dealt with later.

Lower level alerts are not discarded. In a robust solution, they will be analysed to uncover any concerning patterns and trends. For example; a child searching online for 'cotton wool' and then later chatting on Facebook Messenger about 'diets' could indicate an eating disorder which, without the system's trend analysis, may go undetected.

Third-party human moderated - The other type of monitoring is one that is human moderated. In this more advanced solution, a capture is made in the same way as before. Artificial Intelligence (AI) then analyses the capture and creates a profile of the alert context. It also removes false positives at this point.

The capture is then sent to a human moderator for analysis. The analyst grades the capture and decides on the severity of the alert. They will also remove any further false positives.

You are promptly notified of any severe alerts, whereas alerts with a lower severity are sent to you via a scheduled report.

Most providers have a safeguarding portal for you to log in and see the full context of the alert, as well as gather any extra evidence you may require.

Key differences between the two types

Non moderated:

- Lower cost
- Allows your school to create your own individual settings
- Uses risk grading
- Works offline
- Has a console that makes it easy for schools to access and analyse information.

Ideal for: Schools whose DSL is dedicated and has more time to carry out risk assessments.

Third-party human moderated:

- AI profiling creates a clear picture of the context of an alert removing many false positives
- A human moderator - a team of experts - will check your school's captures and analyse their priority grade whilst removing any false positives that may have slipped through
- Is a much more time efficient monitoring solution.

Ideal for: Schools whose DSL is juggling other responsibilities and needs the extra help.

Contact us.

If you have a question or would like to arrange a free demonstration, contact us.

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

3.0 Presenting the Need for Change

With definitions clarified, another important first step is to explain exactly why your organisation needs a monitoring solution.

Identifying where your school is failing to meet its statutory obligations is a key part of this. These concerns will be individual to your school but may include:

- You do not effectively risk-guard vulnerable children sufficiently (a group that are more likely to type than voice their current concerns).
- You do not comply or only partially comply with the changes and expectations in KCSIE 2018.
- The negative impact the issues of the online world are having on pupils' overall achievement.
- Your IT systems are not effectively being monitored and some incidents are slipping through the net.
- You are missing concerns in some students. You might be able to discover risks you are not aware of.
- Your current processes around contextual safeguarding.

The following checklist can help you evaluate your current monitoring provision in more detail and identify where, if any, your gaps may be.

3.1 Evaluating your current monitoring provision

You may find it useful to evaluate your current monitoring provision by drawing up a point score system using the table below. Grading 3 for Effective Monitoring, 2 for Basic Monitoring and 1 for Weak Monitoring, add up what your current monitoring system would score and how an alternative solution would score.

	Effective Monitoring	Basic Monitoring	Weak Monitoring
Policy/set-up			
Age	The system is entirely customisable and can be set to respond to different age groups.	The system has some customisation features between year groups.	Students have restricted access and only use safe features / teacher supervises for appropriate age groups.
Monitoring policy	An acceptable use policy is used and embedded in the culture of the school. It is also used for the purposes of teaching online safety.	An acceptable use policy is used with all students.	Students are told what they should do when accessing the Internet.
Devices	The system can monitor all school devices and BYOD.	Has the ability to work on all managed devices in school.	Only works on desktop computers / only physical monitoring used.
Processes			
Prioritisation alert management	Intelligent analysis and profiling is used to gain a full picture of a student. Added human moderation will ensure only the real risks get through and with the correct severity level.	Schools can customise their risk-grading and words to fit the cohort. They can customise by class groups to avoid curriculum captures.	Customisation is not possible and no profiling or AI exists / only physical monitoring used.
Languages	Supports all languages used in school.	Supports most languages in school.	Limited languages covered / only supervised by teacher over shoulder.
Procedures			
Reporting and evidence	A full contextual background can be viewed in a report. Peer trends or pupil profiles can be analysed.	Context is given with screenshots as evidence.	Logbooks take a lot of time in making sure nothing is missed. Limited evidence is given. No context / teacher reports incidents for DSL to note down.
Data storage	Data is held in a guarded off-site setting with robust levels of online protection.	Data is held in a secure setting with good online protection.	Data is held physically on site and has no additional security restrictions.

	Effective Monitoring	Basic Monitoring	Weak Monitoring
Impact			
What is the outcome and impact of your monitoring strategy?	Alerts are risk assessed in real-time through AI and human moderation. False positives are removed and DSLs only have to react to real alerts.	Alerts are listed in risk order. Relies on the DSL checking through alerts. Gives text evidence.	Alerts are not acted upon promptly enough. Evidence is very limited / teacher may not see misuse or risks as children are good at concealing screens.
Suitable for			
Size of institution / staff / student ratio	Larger settings dealing with many students and where staff time is limited. System uses profiling, AI and human moderation to make sure a school doesn't miss anything important.	Settings where a DSL has the time to go through alerts and do not need much evidence to take action.	Small settings in which students work in very small groups or have extra supervisory staff / TLAs.
Restrictions			
Any limitations	May have fewer customisation options. Not controlled completely within the school.	Will take more time in removing false positives and may not give enough evidence to take action.	With hundreds of students, checking log files or over the shoulder of students opens you up to missing risks. You may need technical help in understanding the logs.

3.2 Your policies and online safety / risk checklist

When assessing your gaps it's important to ensure that all risks that could be created or found in the digital environment are identified and mitigated.

In your organisation's risk assessment and child protection and safeguarding policy, you will find many factors that are digital-specific.

Check through your list and suggest additions if you do not feel all have been highlighted. Depending on your current setup, this may involve school devices in and outside of school. Remember, your digital environment is not just online. You may find peer on peer abuse occurs within school applications. Emails and web chats can also highlight risk concerns.

Online safeguarding will likely be mentioned in your school behaviour policy, your acceptable use policy and perhaps your social media policy. Overall, the most comprehensive guide of your digital safety should be within your school's online safety policy. You will need to check that this policy is up-to-date and covers all risk factors experienced in a modern-day organisation.

This online safety policy helps to show school leaders and governors:

- What their responsibilities are.
- The different aspects that need to be thought about when looking at your digital strategy.
- A clear guide to all members of your school community as to their roles and responsibilities in relation to digital safety.
- A clear understanding of the measures needed to be put in place to safeguard everyone in your community.

360 Safe is recommended in KCSIE 2018. This online safety policy template is created in partnership with 360 Safe.

It might be helpful when reflecting on the above points to give some examples of where you think your online safety and risk detection could have been improved by using active monitoring. This could be real events that have happened in your school or risk scenarios for which you feel your school isn't currently prepared.

Examples

Hayley was a victim of cyberbullying for over 6 months. We only became aware of it when she started refusing to go to school. We are working with her family and other support services to try and persuade Hayley to return to the school setting, but as of yet, we have been unsuccessful. If we had identified this issue earlier, we might have been able to intervene much sooner and it may not have led to this current situation.

Headteacher, 2017

or

Last month, Simon left school to buy drugs during break time. We only found the email after looking through his account post incident. If we had seen that an email was sent to arrange a meeting at break time with an outside person, we may have been able to stop this from happening and have intervened before he was expelled.

DSL, 2018

3.3 External factors that impact on your ability to safeguard effectively

Depending on your current monitoring arrangements, you may wish to highlight some external factors that might impact on your active monitoring capability.

These will be unique to your organisation, but some suggestions include:

Limitations of teaching staff: It is difficult for staff to monitor every screen in a class unless they have a 1:1 ratio. It is very expensive to have extra staff in the classroom to create the appropriate ratio required in this context. The added pressure for teachers to effectively identify risk can place unnecessary strain on their teaching and may even cause them increased stress in their role.

DSL's time pressure: With a system already installed, you could highlight how many safeguarding logs / captures you are receiving a day and how this is making significant demand on the DSL's time.

Technical staff: If your current monitoring provision requires your IT team to monitor captures you can highlight the weight of this responsibility on top of all the other technical demands in the school. If they were to miss a concern to pass on, your DSL would ultimately have responsibility for this. You could point out the benefits of using this time more effectively and how a more efficient workload could provide a cost saving.

Contextual safeguarding: Being able to see risk concerns through email, online chats and documents will help you to create a much wider context of your pupils' lives as a whole and how peers may be affecting them.

Pupil performance and behaviour: By picking up more risk concerns and detecting issues at an early stage, your school performance is likely to improve as pupil issues will be tackled before they escalate.

4.0 Highlighting Areas of Non-compliance

Your stakeholders may wish to understand where your school's weaknesses or gaps are in meeting monitoring legislation and guidelines.

A way for you to show this is by creating a table (see below). This table includes the sorts of examples you might cover but will of course be relative to your school.

KCSIE legal requirements	Weak Monitoring	Effective Monitoring
Illegal content	We cannot ensure our students aren't accessing illegal content.	Active monitoring uses advanced keystroke and screen-view technology. Even if a student accesses illegal content, the DSL will be alerted to such behaviour.
Mental health	Our filtering system does not communicate captures to the DSL in real-time. If a student has shown signs of being suicidal, we may never know or there is a delay in us finding out.	Active monitoring works in real-time and will alert the DSL rapidly. We will be able to act on the information promptly and implement our child protection procedure.
Radicalisation	The government has raised concerns that extremists are able to communicate through encrypted connections. Filtering will not always block these connections.	Some active monitoring solutions are not defined by VPNs therefore keystroke and screen-view technology would also pick up any conversations if they showed signs of radicalisation.
Child sexual exploitation	Our current system does not pick up an email with phrases such as "don't tell your parents".	An active monitoring system would pick up on emails of an adult-child nature where an abusive or exploitative concern is shown.
Discrimination	We currently do not pick up on digital activity which involves discriminative actions / text.	Active monitoring would pick up and alert us to such activity and regardless of the application used, give us clear evidence to follow it up.
Drugs	Our current monitoring system is not responsive to our students' code words for drugs.	An effective active monitoring solution would use up to date language and could allow us to add code words to our monitoring system.
Bullying	Our current monitoring system would not pick up peer on peer abuse in collaborative documents or web chat.	A good solution would pick up issues out of the browser and encrypted sites.
Violence	Our current monitoring solution doesn't work in real-time. If monitoring discovers a student has a knife, we need to know straight away.	An effective monitoring solution would send a severe alert straight away for this kind of instance.
Self-harm	Our current monitoring solution often flags the word 'cut' as self-harm. This causes many false positives which wastes a lot of time to check through.	An effective human moderated monitoring solution would remove these false positives or risk-grade them more effectively.

5.0 Emphasising Your Statutory Obligations

Once you have clarified your gaps, it's important to explain / remind stakeholders of your school's statutory obligations to address them.

Many schools and their stakeholders still have a limited understanding of what's required from Ofsted. If that applies to you, download Smoothwall's 'A School's Complete Guide to Monitoring' for more help (see page 23).

With the provision for monitoring only becoming a requirement in 2016 and the issues of the digital age only given full prominence in the last couple of years, many schools are at different stages in their monitoring journey.

It is important to remember that monitoring is essential for determining students at risk. It not only shows you when students access material they shouldn't, but it is also there to pick up behaviours that are indicative of an issue.

The following references give clarity around your organisation's accountabilities:

The Prevent Duty 2015

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school".

KCSIE 2018

"Ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school's IT system," however, schools will need to "be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

- Schools should be able to identify signs of abuse or neglect.

"All staff should be aware of indicators of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection. Knowing what to look for is vital to the early identification of abuse and neglect."

Active monitoring is able to identify risks to staff and will highlight the category of the type of concern it has identified. It acts as an extra guard for teachers that may not have spotted other signs.

- A clear strategy on early help.

In the monitoring context, the rapid identification of concerns means that schools are alerted to issues at an early stage and can intervene early.

- Schools need to make sure they are acting rapidly to signs of an issue. They should check that no factors could put this strategy at risk.

"All staff should be aware of their local early help process and understand their role within it."

A good active monitoring system will work in real-time and send alerts to the safeguarding staff on duty at that time. Alerts going straight to the safeguarding lead means no time is wasted by staff handing over information, or through systems where you have to trawl through lots of data and reports.

"It is important for children to receive the right help at the right time to address risks and prevent issues escalating. Research and serious case reviews have repeatedly shown the dangers of failing to take effective action."

Examples of poor practice include:

- Failing to act on and refer the early signs of abuse and neglect
- Poor record keeping
- Sharing information too slowly
- Schools need to show that they are protecting SEN and disabled students. It has been identified that this group are particularly vulnerable in the online space as they are less likely to communicate their actions effectively. Their digital behaviour is likely to give a school a wider picture of their safeguarding needs.

As a reinforcement of your organisation's accountabilities you could also explain the concerns you should be monitoring for (as outlined in KCSIE):

Abuse - Online abuse may be an extension of abuse happening in the 'real world' or it may be only occurring online. It could be from peers or outside of school.

"Abuse can take place wholly online, or technology may be used to facilitate offline abuse."

Emotional Abuse - Emotional abuse involves an attempt to control. For instance, emotional abuse could involve one parent threatening a child if they contact the other parent.

"It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying)."

Sexual Abuse - Online sexual abuse can occur in many ways.

"Non-contact activities, such as involving children looking at, or in the production of sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse."

Peer on peer abuse - Sharing of videos from events or taunts online about another child's preferences. This area has become an increasing problem in schools.

"Cyberbullying and sexting (also known as youth produced sexual imagery)." The school child protection policy should show how schools are minimising the risk of peer on peer abuse.

SEN and disabled students' extra risk - Schools must ensure they have an effective system for identifying vulnerable SEN and disabled students online.

There is "potential for children with SEN and disabilities being disproportionately impacted by behaviours such as bullying, without outwardly showing any signs; and communication barriers and difficulties in overcoming these barriers".

Protecting victims of sexual harassment or abuse - A common problem for schools is peer to peer youth produced sexual imagery.

Schools have a duty to be monitoring for any of these behaviours. They also have a duty to protect a victim from any malicious bullying after a complaint has been made.

CSE (child sexual exploitation) - The occurrence of CSE can take place across all backgrounds. Children are sexually exploited for power, money or status. It can seem to start as a normal relationship and quickly lead to being forced into something they do not want to do.

It "can take place in person or via technology, may occur without the child or young person's immediate knowledge (e.g. through others copying videos or images they have created and posted on social media)."

Gangs and youth violence - Often the only sign a school might come across indicators of youth violence is in the digital environment. Schools need to be alert to signs and look for identification markers such as peer to peer bragging or contextual information.

"Inspections will include a consideration of pupils' ability to assess and manage risk appropriately. This explicitly includes online safety, substance misuse, knives and gangs, and relationships (including sexual relationships)."

Radicalisation - In order for schools and childcare providers to fulfil the Prevent duty, it is essential that staff are able to identify children who may be vulnerable to radicalisation.

"Radicalisation can occur through many different methods (such as social media) and settings (such as the Internet)."

Suicidal thoughts - Often when children are feeling suicidal, they will look for avenues of help that do not include involving other people. Searching for help often occurs online or may be expressed in written word documents and notes in the digital realm.

Other areas schools are expected to monitor for include drugs, self-harm, discrimination and pornography.

6.0 Which Monitoring Solution and Why?

Your stakeholders may expect you to have a view on what solutions are available on the market. It's helpful to know what's what and be ready to answer any questions from an informed perspective.

When evaluating monitoring providers, it is advisable to check their response to the UK Safer Internet Centre Provider Response Form. In line with the recent changes to the guidance, the UK Safer Internet Centre issued a more informative form for providers to respond to back in June 2018.

The first part of the form checks that the provider's solution monitors for (as a minimum); illegal, bullying, child sexual exploitation, discrimination, drugs / substance, extremism, pornography, self-harm, suicide and violence. The second part checks how the provider's solution does this.

Overleaf is a handy checklist along with suggested granular questions to help short-list potential monitoring providers.

Smoothwall offers both moderated and non-moderated monitoring solutions

For an informal discussion or to arrange a demonstration, contact us on:

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

To see the Smoothwall responses to the UK Safer Internet Centre Provider checklist, visit www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-responses-1

UK Safer Internet Centre - How does the monitoring system meet the following principles?

Additional questions

Age appropriate	Includes the ability to implement variable monitoring appropriate to age. This will, in turn, define which alerts are prioritised and responded to. Further situations may warrant additional capability, for example boarding schools or community-based access.	Check to see if the solution gives you detailed settings based on age / class group.
Alert management	How alerts are managed? Whether schools manage system alerts or support / management is provided.	Look at how alerts are made available. Do they go to the DSL in real-time? Are they checked by risk grading, AI or human moderation to ensure alerts are effective?
BYOD (Bring Your Own Device)	If the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the school), how is this deployed and supported, and how is data managed? Does it monitor beyond the school hours and location?	Check for what a BYOD system can actually cover.
Data retention	What data is stored, where is it (physically) stored and for how long?	Check the security your provider offers when protecting your sensitive data.
Devices	If software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers.	Check which devices the provider covers.
Flexibility	The schools' ability to amend (add or remove) keywords easily.	Check you are able to customise your data if you are handling full management in the school.
Group / multi-site management	The ability for deployment of central policy and central oversight or dashboard.	Check if there is a central dashboard and options for scalability.
Monitoring policy	How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	Check the provider's suggested acceptable use policy.
Multiple language support	The ability for the system to manage relevant languages.	Can the provider check all languages used in your school?
Prioritisation	How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?	Will the provider's solution work in real-time and give you a priority level?
Multiple language support	How are alerts recorded within the system?	Does the provider give contextual screenshots or build a profile?

7.0 Additional Benefits of Active Monitoring

There are a number of additional benefits you may also wish to include in your case.

Open Internet

Having an effective active monitoring solution in place helps create a wider learning environment for pupils in your school. You can safely make some aspects of the Internet, such as social media, more accessible therefore creating a more enriching and accessible learning environment for your students.

Teaching tool

A new requirement in KCSIE 2018 is the need to teach students how to use the online world in an effective and safe way.

The education for a connected world framework identifies the need to explore different online aspects including bullying, privacy and security, online relationships and more. By using the technology that students use at home for these concerns, students can explore the specific ways to stay safe at school.

Giving students the power of their own responsibility has been shown to be one of the most effective ways to make sure they are protected online.

8.0 Sources of Funding

With schools expected to face real-term cuts in spending per pupil, finding funds for systems not already in place can be challenging.

Many schools will see monitoring as part of their IT budget. The question then arises as to whether a school should really be competing for a share of a budget over an upgrade of a computer room, or a new piece of software for a department against their school safeguarding strategy.

You may wish to highlight that monitoring is purely for the safeguarding of students, therefore a more suitable budget may be one from the school's safeguarding or general fund. You could also emphasise, depending on the solution you choose, that a different solution could save staff time and therefore impact minimally on overall cost.

It could be that you need to suggest an extra means of funding e.g. a crisis / exceptional fund for the first year, and then make plans as to how to fit it into the school overall budget the following year.

You could give a range of solutions to show that you have researched this effectively and have different options depending on the budget available. For example:

1st solution - Proactive monitoring. An all-round package that will save staff time and ensure that there is full protection in place.

Cost £

2nd Solution - Active monitoring - budget solution. This requires more staff input to keep an eye on captures. The school's DSL or deputy DSL on duty will need to be on hand to review incoming alerts.

Cost £

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

Safeguard Monitoring: A Complete Guide to Active Monitoring for Local Authorities and Multi-Academy Trusts

What is monitoring, why do Ofsted require it and how can you and your schools integrate it into your safeguarding strategies?

Available at: https://smoothwall.com/active-monitoring-local-authorities-and-multi-academy-trusts

Safeguard Monitoring: A Complete Guide to Active Monitoring for Colleges

What is monitoring, why do Ofsted require it and how can you integrate your college's safeguarding strategy?

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

Whitepaper

Further reading (continued)

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

Web Filtering in Education: Cloud, On-premise or Hybrid?

A complete guide designed to give IT Leaders in Education thorough insight into the many deployment options available to best suit their network needs.

Available at: https://smoothwall.com/web-filtering-deployment

Web Filtering in Multi-Academy Trusts: Cloud, On-premise or Hybrid?

A complete guide designed to give IT Leaders in multi-academy trusts thorough insight into the many deployment options available to best suit their network needs.

Available at: https://smoothwall.com/web-filtering-deployment-mats

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.

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

Contact us

We hope you found this document useful. If you require any help preparing your case for funding or answering any questions your stakeholders may have, please contact us. Likewise, if you would like more information on Smoothwall Monitor or to arrange a demonstration. We'd be delighted to help.

Arrange a free demonstration

To see a free, no-obligation demonstration of Smoothwall Monitor or to ask any questions please contact us.

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

Avalon House,
1 Savannah Way
Leeds Valley Park
Leeds
LS10 1AB

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

smoothwall.com

Smoothwall
Smoothwall
Smoothwall-ltd
SmoothwallTV

smoothwall®