Smoothwall for Education

Whitepaper

Digital Safeguarding

A School's Complete Guide to Active Monitoring

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

smoothwall®

smoothwall.com

Whitepaper

Contents

Appendices

About this document

This document has been produced by Smoothwall's Online Safeguarding Experts to help schools navigate the legislation and recommended guidelines in order to respond in an appropriate way.

It explains what monitoring is and how schools can integrate it into their existing safeguarding strategy. It answers the key questions many schools are asking and shares real case scenarios of monitoring in action.

Essential reading for: Designated Safeguarding Leads, Governors, Headteachers and anyone interested in or responsible for ensuring safeguarding compliance within a school.

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

We'd be happy to help.

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

smoothwall®

1.0 Introduction

For many children in the UK the Internet, computers and mobile devices are all part of everyday life.

The majority of families have at least one connected device in their home, and for schools, the Internet and computers are an everyday component of lessons and learning.

Although technology brings tremendous opportunity, it also brings inherent danger.

Bullying, or peer on peer abuse, in schools is nothing new. Where previous generations of children could go home to safety, the viral nature of their online life means they no longer have a safe place to go. They have no escape. Children and young people can be on the receiving end of humiliating or degrading messages, sexual images or videos 24/7. They can also be exposed to exploitation, grooming, gang membership, radicalisation, gender-based violence, and trafficking.

The result is a surge in the number of children and young people suffering from mental health issues caused by their online activities.

The Office for National Statistics has found a *"clear association"* between longer time spent on social media and mental health problems amongst children. In a recent survey, 98% of teachers or school leaders said they had come into contact with pupils who were experiencing mental health issues, including children as young as four.

Smoothwall's own research has shown that 95% of teachers rely on students to tell them if they are being cyberbullied. But only 5% of children say they will confide in a teacher. That's an alarming disconnect.

Children's safety online is a growing problem and is one of the reasons why the Department for Education (DfE) has introduced, and continues to upgrade, its statutory online safeguarding requirements for schools, including the role of safeguard monitoring.

Although safeguard monitoring was a requirement in Keeping Children Safe in Education (KCSIE) 2016 there is even more focus in the September 2018 update.

"All school and college staff have a responsibility to provide a safe environment in which children can learn. It is essential that children are safeguarded from potentially harmful and inappropriate online material."

It emphasises that schools need to ensure *"appropriate filters and ... monitoring systems are in place"*.

Despite this many schools are still unclear about how to safeguard children through monitoring and the role it must play in their safeguarding strategies.

This document is a practical document to help schools understand and respond appropriately.

95% of teachers rely on students to tell them if they are being cyberbullied. Only 5% of children say they will confide in a teacher. That's an alarming disconnect.

Smoothwall Insights, 2018.

2.0 Changes to Guidelines and Legislation

In this section we review the main legislative and guideline changes and the provision schools must evidence as it relates to monitoring.

KCSIE 2018

- Schools and colleges in England are obliged to *"ensure appropriate filters and appropriate monitoring systems are in place"*.
- Monitoring systems are there to safeguard children and the responsibility should lie with the school leadership/ Governors and Designated Safeguarding Lead (DSL).
- Monitoring systems require capable and competent staff to sufficiently manage them, together with the support and knowledge of the entire school.
- Schools must have their own safeguarding policy based on their setting and needs. This means identifying the risks most specific to them and showing how they effectively intervene and help students when a problem arises. Even schools within a multi-academy trust are now expected to have their own individual policy.
- Assessments of children should consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare.
- DSLs to likely have a *"complete safeguarding picture"*.
- The DSL should take lead responsibility for safeguarding and protecting children, including online safety.
- DSLs must be up to date in training for online safety.
- They must understand the vulnerability of children with SEN and disabilities in the online environment – with everything from online bullying, to grooming and radicalisation.
- DSLs must be confident they have the capability to support SEND children to stay safe online.
- DSLs should understand the risks associated with online safety and be confident they have the relevant knowledge and up to date capability to keep children safe whilst they are online at school.
- Data protection and GDPR should not interfere with the ability to share information relating to safeguarding.

  "The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children".

Working Together to Safeguard Children 2018

- Communication between schools and multi-agency safeguarding partners is crucial.
- Clear evidence and a full picture will help the agencies put the right measures in place.
- Schools should provide support as soon as a problem emerges to avoid escalation.
- Local organisations and agencies should have in place effective ways to identify emerging problems as well as potential unmet needs of individual children and families.
- All practitioners to understand their role in identifying emerging problems and to share information with other practitioners to support early identification and assessment.

OFSTED

- Inspectors should be able to see evidence of how a school is safeguarding children appropriately in the online environment.
- Schools should have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe.
- Inspectors should consider the extent to which leaders and managers have put in place effective arrangements to identify children and learners who may need early help or who are at risk of neglect, abuse, grooming or exploitation.
- At all times the school or college should be actively considering the risks posed to all their pupils and students by putting adequate measures in place to protect them and keep them safe.

The UK Safer Internet Centre

This guidance highlights that schools should be led by their own risk assessments when deciding what level monitoring is right for them. All schools must be able to show how they monitor for and protect against:

- **Bullying:** Any behaviour that includes threats, coercion to abuse, intimidation or aggression towards other students.
- **Child sexual exploitation:** Manipulative or coercive behaviour towards a child that encourages them to engage in a sexual relationship, including encouraging to meet.
- **Discrimination:** Any prejudiced or unfair behaviour that defies the Equality Act 2010.
- **Drugs / substance abuse:** Any evidence of drug misuse or promotion of illegal drug use.
- **Extremism:** Content that encourages terrorist or terrorist ideologies, including intolerance or signs of violence.
- **Illegal:** Any content that is illegal. For example, extremist content or child abuse images.
- **Pornography:** Content that includes explicit imagery or sexual acts.
- **Self-harm:** Content that encourages or exhibits deliberate self-harm.
- **Suicide:** Anything that might suggest the user is considering suicide.
- **Violence:** Any threat or sign of physical force intended to hurt or kill.

The Prevent Duty 2015

- Schools should be aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the Internet. Schools and childcare providers should have *"clear procedures in place for protecting children at risk of radicalisation"*.

3.0 Meeting the Guidelines and Legislation

The challenges for schools

Schools are now under more pressure than ever to keep tabs on how pupils are interacting online.

With class sizes often more than 30, identifying every risk may feel like an impossible task, especially for a busy and often overstretched school. And these risks are not going away.

The online risks to a child's safety and well-being are increasing all the time.

Mental health

10% of school children have a diagnosable **mental illness**

Source: Mental Health Foundation

Peer on peer

64% of girls aged 13-21 have experienced some form of **sexual violence or harassment** at school

Source: Children and Families Minister at Safeguarding Conference - 2018

Abuse and grooming

700% rise in **online sexual grooming**

Source: Home Secretary Sajid Javid, Home Office

Suicide

107% increase in **suicide** between 10-19 year olds in London, UK

Source: ONS

Bullying

1 in 5 students have been **bullied** in the last year

Source: Annual Bullying Survey

Self harm

68% rise in **self harm** in girls

Source: NHS UK

Only one in eight children in England who are sexually abused come to the attention of statutory authorities.

Ofsted. 'Guidance for joint targeted area inspections: child sexual abuse in the family environment.' August 2018

Schools are often in the dark to what is happening

The universe has shifted for today's young people. They do not perceive the online world as separate to the offline world. Social media is an ever-present consciousness in their lives. A constant obsession to obtain the most streaks or likes can mean that young people are prepared to expose themselves to unknown contacts and therefore immense risk.

Unfortunately, in the online world there is no undo button. Incidents outside of school may impact on the environment inside the school and visa versa. From hurtful messages to sharing images, schools can struggle to keep up and are often in the dark to what is happening.

Vulnerable, SEND and disabled students are at particular risk. KCSIE reminds schools to always have an *"it could happen here"* approach.

The move into secondary school has been identified as another risk. It's a time when students disregard their previous online safety advice and start to have the mentality 'it won't happen to me'.

Serious risks are often shared online, whether it be a student with knife possession, a student who is hours from suicide, or a student about to engage in illegal drug use, sometimes the only hint of this happening may be through their use of technology.

With high risk comes the need to detect and react fast, and without an active monitoring solution, schools are unlikely to meet their legal obligations or duty of care.

The long-term impact if risks are not identified

A report published in July 2018 by the UK Mental Health Policy Commission shows evidence that adverse childhood experiences can lead to mental health issues. By the age of 15, 50% of mental health issues will already have been seeded. Early intervention through active monitoring can reduce this significantly.

The imperative for schools

KCSIE, Working Together to Safeguard Children and Ofsted's Inspection Guidance all emphasise the need to proactively identify problems and concerns and to have in place a core strategy for risk prevention and early intervention.

Schools must review whether they are using the most effective solutions to identify students in need.

Technology based active monitoring solutions enable schools to identify risks that may otherwise go unnoticed. They give a deeper picture of issues and concerns, alert you to issues at an earlier stage and provide you with clear-cut evidence that's vital when working with external agencies and partners to ensure young people get the support they need.

The fact is your school will not meet its obligation while it remains unaware of troubled students or students at an early stage risk.

Identifying at risk students is now the task at hand for schools across the UK. And the good news is that technological advances in safeguarding and active monitoring make this easier than ever before.

4.0 The Role of Active Monitoring

What is 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 to check for signs of risk in children.

Helping identify risks

Active monitoring helps you to identify students at risk quickly. Serious risks such as a suicide, grooming, or a gang meeting can all be picked up in real-time if a child has used their keyboard 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'.

It can help you detect problems and respond to issues you were previously unaware of and help individuals who haven't previously been shown to be at risk. For students 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.

How it works

There are generally two types of active monitoring solutions available:

1. **Non third-party moderated**
2. **Third-party human moderated**

Non-third party 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. This capture could be of a browser, an email, a Microsoft document, a social media platform or a chatroom. Active monitoring is not like CCTV that films everything. It only captures moments where a person has shown risk.

The system will create a risk-grade based on the capture. Schools can see risk alerts easily enabling them to act on severe alerts immediately.

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.

Severe alerts are immediately sent to you and lesser alerts may be sent in conveniently timed reports.

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

> Identifying students at risk is now the task at hand for schools across the UK. And the good news is that technological advances in safeguarding and active monitoring make this easier than ever before.

Social Media and School Crises National Association of School Psychologists

Key differences

Non third-party moderated

- Lower cost
- Allows your school to create your own individual setting
- 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 more time efficient monitoring solution as most false positives will be removed.

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

Do you have a question?

Contact our online safety experts. We'll be happy to help.

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

Helping identify risks - real case scenarios

The following cases show how monitoring can help you identify risks. These scenarios are based on real stories although the names and details have been changed to protect confidentiality.

Monitoring type: **None in place**

Bobby year 9

Risk type:
Violence to others

1. Bobby brought a knife into school.

2. He messaged one of his peers that he was going 'to get' Mrs Browning.

3. Later that afternoon, Bobby stabbed Mrs Browning.

4. The log was found the next day by the school technician, after painstaking forensic analysis of the computer Bobby was using.

5. If active monitoring had been used, this risk would have been spotted and the stabbing avoided.

Freddie year 9

Risk type:
Drugs

1.Freddie was working on a shared document with a friend.

2. Freddie quickly typed in *"fancy a spliff at break?"*. The friend agreed and then deleted the words.

3. At break-time, Freddie and his friend met up and smoked cannabis.

4. The use of drugs was discovered several weeks later by a member of the break-time staff.

5. If active monitoring had been used, this incident would have been spotted and the drug-use avoided.

Jessica year 8

Risk type:
Cyberbullying & self harm

1. Jessica moved in the middle of the school year and was having trouble fitting in.

2. She became depressed and began a Word document on her computer as a diary.

3. As her depression worsened she read a forum online about depression and began to cut herself.

4. She covered her arms and legs for weeks to hide her self-harm. It wasn't until her PE class started gymnastics that her teacher noticed the scars.

5. If digital monitoring had been used, this risk could have been spotted and she could have received treatment.

Monitoring type: **Non third-party moderated**

Emma year 6

Risk type:
Child exploitation-vulnerable student

1. Emma was sat at a school computer during her lunch break.

2. She was sent a threatening email saying that if she didn't meet someone called Richard after school, he would post the photos she sent to him so that everyone could see what she had done (using serious sexual language). She was told *"not to tell anyone"* about the meeting.

3. The serious sexual language triggered a severe alert.

4. The school DSL picked up the alert. She was able to intervene by asking Emma to come and talk to her.

5. The DSL invited Emma's foster parents into the school and used the support of her social worker and outside agencies to help Emma. Richard was reported to the Police and the school were able to give clear evidence of the incident. The monitoring system de-escalated the problem and ensured Emma received the help she needed.

Matthew year 7

Risk type:
Violence

1. Matthew was in a maths lesson where the teacher had set a 20-minute maths consolidation exercise on the computer.

2. While his teacher helped another student on the other side of the classroom, Matthew wrote a note on screen,*"I think James brought in a knife"*.

3. An alert was triggered at this point and sent to the school's DSL. Matthew nudged his best friend to take a look. His best friend saw it but then Matthew's maths teacher called the class to attention. Matthew quickly deleted the note on screen.

4. The school DSL on duty had seen the alert and its severity. Having a full safeguarding picture of the school the DSL knew which James the note was referencing. They de-escalated the situation by implementing the school safeguarding strategy to remove weapons from a student.

Sara year 9

Risk type:
Peer on peer bullying

1. A relationship rift had caused a group of girls to set-up a *"we hate Sara Potts"* website.

2. The girls posted malicious messages anonymously on the website with cruel comments.

3. Sara told a teacher but didn't know who was doing it.

4. The school added customisation around Sara Pott's name on the website. The DSL received alerts of 5 girls adding to the website within 24 hours and could follow up on the situation.

Monitoring type: **Third-party moderated**

Sabena year 10

Risk type:
Discrimination

1. Sabena had created a video of her classmate Sophie and had placed Sophie's head on a dog's body. Sophie had Marcus Gunn Syndrome.

2. Sabena set-up a website called *"Sophie, the dog"*.

3. Sabena's friend Thea accessed the website from her Chromebook and wrote *"yeah Sophie looks good as a bitch"*.

4. An alert was triggered and sent to the human moderator.

5. The human moderator assessed the situation and notified the school.

6. The DSL logged into the monitoring console to see the full context. The DSL was able to immediately implement the school safeguarding policy for this context.

Mohammed year 11

Risk type:
Suicidal

1. Mohammed typed into Google *"the most pain free way to kill yourself"*.

2. Although never pressing Enter, his keystrokes were recorded and an alert was sent to the human moderator.

3. The human moderator could see how Mohammed had previously looked up paracetamol and codeine. They contacted the school's DSL immediately.

4. The Safeguarding Lead logged into the console, located Mohammed's whereabouts and put together a swift plan to implement the school's safeguarding policy for a child at risk and intervene before it was too late.

Harry year 5

Risk type:
Self harm

1. Harry typed into Google *"short haircuts"*.

2. An alert was raised for self-harm because of the word 'cut'.

3. AI and human moderation removed this as a false positive.

Active monitoring with a human moderator allows you to act on alerts fast, as well as save time by removing false positives like the one above. A good proactive provider will build individual profiles and learn from past experiences to have a clear understanding of your cohort.

Helping you meet Ofsted requirements

Ofsted now asks you to provide evidence of appropriate monitoring.

Active monitoring provided by a technology-based solution helps you meet Ofsted requirements in a number of key ways:

- Identify individuals at risk, (both obvious and not so obvious) allowing you to intervene early and provide support as required.
- Highlight risks and concerns in real-time giving DSLs a comprehensive picture of the risk landscape affecting their school.
- Demonstrate far reaching effective arrangements to identify children at risk.
- Give you a full evidence-based picture of your safeguarding provision as well as communicate effectively to outside agencies and ensure those at risk are identified and receive the right support at the right time.
- A high quality monitoring solution will expand your safeguarding provision whilst reducing the number of false positives, supporting and facilitating, not adding to, existing resource requirement. (A human moderated monitoring solution removes false positives almost entirely.)

Evaluating your existing monitoring system

	Green	Amber	Red
Policy/set-up			
Age appropriate	The system is entirely customisable and can be set to respond to different age groups.	The system has some customisation 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 into the culture of the school. It is also used for the purposes of teaching online safety.	An acceptable use policy is applied to all students.	Students are told what they should do when accessing the Internet.
Devices	The system can monitor all school-owned devices and BYOD.	The system can support all managed devices in school.	Only works on desktop computers or only physical monitoring used.

	Green	Amber	Red
Processes			
Prioritisation alert management	Alerts work in real-time and enables the DSL to address concerns when needed immediately. They are activated by various sources, both online and offline.	Alerts are risk-graded but safeguarding staff are not notified in real-time. Alerts may not appear outside of the browser. The system may be limited in the way it makes captures.	DSL must look through a logbook for any issues. Limited or no prioritisation. May have limited categorisation / teacher makes note if they see an incident.
Flexibility	Intelligent analysis and profiling is used to gain a full picture of a student. Added human moderation will ensure only the right risks get through and with the right 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.
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 time to ensure nothing is missed. Limited evidence given. Relies on busy teachers to report activity.
Monitoring policy	An acceptable use policy is used and embedded into 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.
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.
Impact			
What is the outcome and impact of your	Alerts are risk assessed in real-time through AI and human moderation. False positives are removed and DSLs only have to react to genuine alerts.	Alerts are listed by severity level. The system relies on the DSL to review alerts. Gives text evidence, no screen captures.	Alerts not acted upon quickly enough. Evidence is 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 for a disciplinary.	Small settings in which students work in very small groups with simple networks or have additional extra supervisory staff / TLAs.

5.0 Integrating Active Monitoring into a Busy Safeguarding Strategy

It's important when implementing a monitoring solution that it integrates effectively and efficiently into your current safeguarding procedures plan.

Failure to do so can cause conflict and stress within your practices which can lead to non-compliance, risks being missed and the ultimate compromising of a child's safety.

The following are key points to consider in order to choose the right solution and ensure a smooth integration.

Integrating with your safeguarding processes

- Will the monitoring solution fit into your processes identifying students at risk?
- Will it be easily accessible to the safeguarding lead so that they can determine levels of risk quickly and efficiently without missing major concerns?
- Check the solution's features will effectively risk grade and categorise the type of risk that has been flagged.
- Does the solution allow you to react quickly to concerns? Ask how long it takes for an alert to take place. Ask whether it functions in real-time.
- Does it include online and offline captures, for browsers, email, Microsoft documents and chatrooms?
- Alerts are just as likely to come in a Word document as they are from the more obvious chat room or email. Not having this level of reach will impact on your ability to spot risks.
- Ensure your system monitors multiple languages if needed.

Integrating with your safeguarding procedures

- Once a pupil at risk has been identified check that your monitoring solution supports the procedures that follow.
- Does it provide evidence and detail to share with parents or outside safeguarding bodies?
- Does it give context around a capture to enable understanding of the full picture?
- Is it age appropriate? Check that it allows for different levels and content settings dependent on your year groups and curriculum sets. This will help in prioritising your alerts and avoiding false captures.

Integrating with your safeguarding policy

- Will the monitoring solution you choose help you to pick up signs of issues from various contexts whether it be a third-party contacting by email or webchat, or peer to peer digital communication?
- Will it give you a better understanding of risks that may not involve time in school or at home?
- A good monitoring solution will not invade privacy. It will pick up risk concerns that should be identified, as outlined by KCSIE guidelines.
- Can it provide easy customisation so that you can manage risks local to your individual school?
- Check that you are aware of how long your data will be stored and whether it is kept in a secure setting.

6.0 Commonly Asked Questions

How much should we expect to pay for monitoring?

Active monitoring solutions range in price depending on the number of pupils, the quality and range of monitoring, whether it is real-time risk grading, moderated by humans or AI, and other factors. Most good providers, like Smoothwall, will offer a number of different solutions to match your requirements and budget.

How are other schools budgeting for this?

Sources of budget varies from school to school. Since the DSL has lead responsibility for online safety under their school safeguarding remit, some schools may choose to fund it from their risk / safeguarding budget, whereas others might use their general / ICT fund. If this is a new addition to include in your school budget, you may need to request funding.

Smoothwall have written a document to help prepare a case for funding. You can download at https://smoothwall.com/how-to-create-a-case-for-funding

How can we use active monitoring within the Data Protection Act 2018 and GDPR?

Monitoring is not affected by Data Protection Act and GDPR. KCSIE 2018 states:

"The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children."

How do we know that a monitoring system will store our data securely?

You will need to ensure the safety of your sensitive data. Vendors should be able to show evidence of where your data is stored. At Smoothwall, data privacy is a top priority and data is stored in a secure Microsoft Azure data centre. Smoothwall employees are DBS checked, even those who don't visit schools.

How can we check the impact a monitoring solution might have on our school's IT systems?

You should check with your vendor that their software is discreet and that you have the necessary capacity required to run it on your school network. All Smoothwall's monitoring solutions have no discernible impact on performance and work silently in the background. A user will not be aware that monitoring is taking place or that a capture has been taken.

What's involved in implementing a monitoring solution?

Installation can be different depending on the vendor. Ask if there is a requirement for staff to have specific technical knowledge and if the system is cloud based. At Smoothwall, installation is simple and straight forward with no technical knowledge required. It can be as easy as flipping a switch, or a simple client download, depending on your current filtering provider.

We already have web filtering, why do we need monitoring as well?

Filtering blocks content to prevent it being seen and accessed by students. It is essential. But it cannot monitor what a child types into their computer. Most filtering systems do not send alerts in real-time enabling you to act upon them quickly. Monitoring and filtering work hand in hand to provide you with a robust digital safeguarding capability that helps you keep children safe and meet Ofsted's requirements.

Our schools are overstretched as it is. Won't monitoring add more safety concerns to address?

Most providers understand this and will offer a choice of solutions to match the level of capacity your school has available. At Smoothwall these range from manual severity risk grading, to saving hours in the week by using AI and human moderation.

Will monitoring make unnecessary captures by topics used in the curriculum?

In some solutions, customisation is available to manage your risk settings so that you can remove key topics for specific classes. However, in doing this you should be careful not to remove content that might need to be there. Every school has different needs which is why a good monitoring system will vary and have flexible settings to suit your environment.

Is monitoring scalable for larger institutions?

If you are a larger institution, it is essential that you check to see how a provider can create a scalable solution. Ask them to explain the timeframe and process of installation. All Smoothwall monitoring solutions are easily scalable due to their minimum impact on networks, cloud-based portal, their easy installation and their automatic updates.

Do you have a question?

Contact our online safety experts. We'll be happy to help.

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

Whitepaper

Appendices

Further reading

You may also wish to download:

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

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

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.

Smoothwall exclusively partners with National Online Safety to offer customers their award-winning e-safety training for the whole school community. We also partner with EduGeek and regularly consult Headteachers, Teachers, DSLs, IT leaders and a range of supporting bodies across UK Education.

Contact us

Ask yourself

Are you confident that you are picking up, in real-time, each of the risk concerns on your school digital devices – online and offline?

If you don't know, it's time to check. If you're unsure or have a question, contact Smoothwall's Online Safety Experts who will be happy to help.

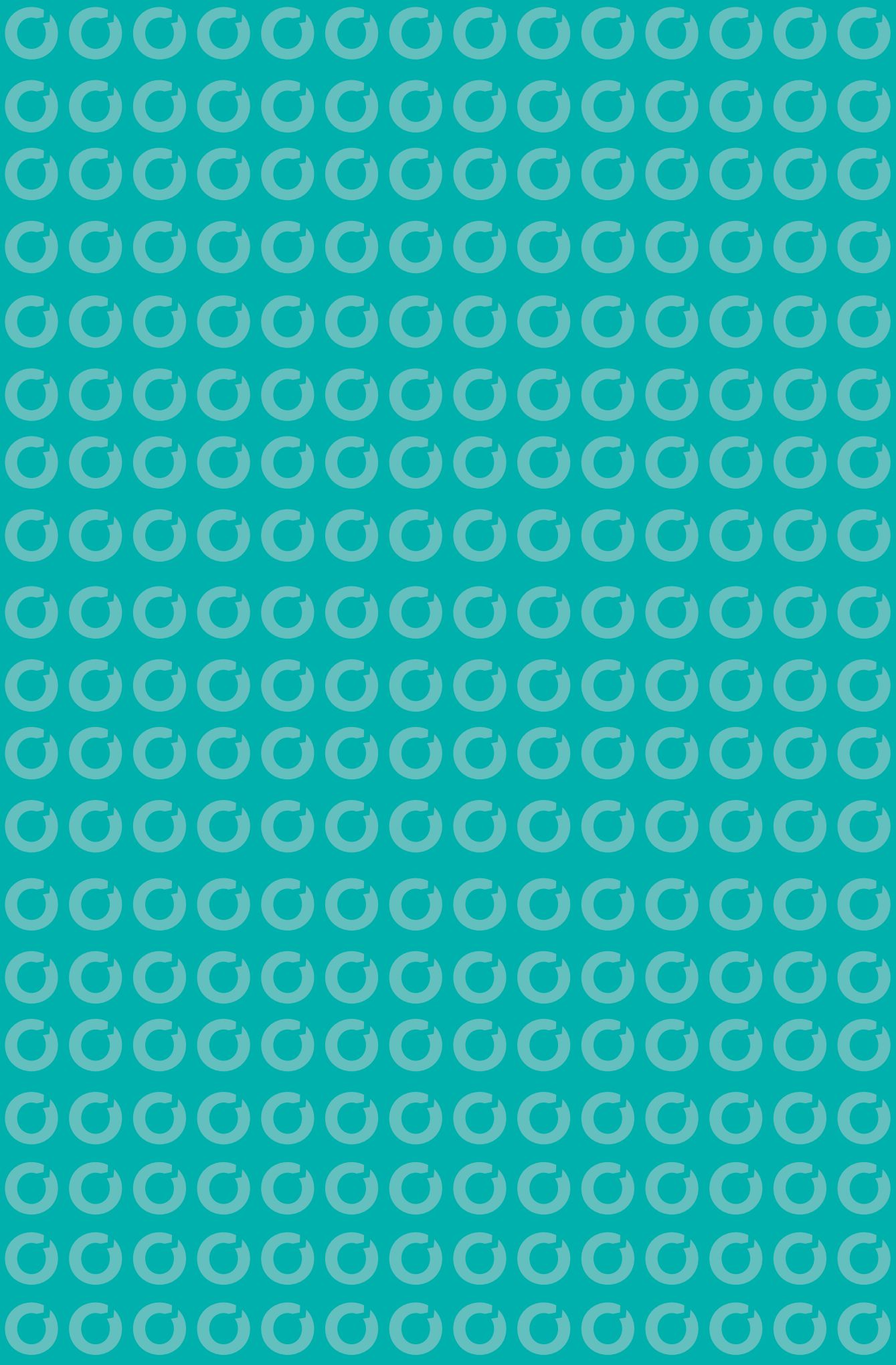
Arrange a free demonstration

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

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

smoothwall.com

smoothwall®



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 Ltd. This document is the copyright work of Smoothwall Ltd 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 Ltd.

smoothwall®