



A Complete Guide to Digital Monitoring for Schools

In this guide: What is digital monitoring and how can it help your school to spot students at potential risk?

smoothwall.com

smoothwall[®]
by Qoria

Contents

1.0 Introduction	04
2.0 Guidelines and Legislation	06
3.0 The Digital Monitoring Challenges Schools Face	11
4.0 The Vital Role of Digital Monitoring	14
5.0 Helping Identify Risks - Real Case Scenarios	17
6.0 Providing Evidence for Ofsted	20
7.0 How to Ensure Your School is Monitoring Appropriately	21
8.0 Integrating Digital Monitoring into Your Safeguarding Strategy	24
9.0 Frequently Asked Questions	26
Appendices	28
About Smoothwall	29
Contact Us	30

About this guide

This document has been produced by Smoothwall's digital safeguarding experts to help schools navigate the legislation and recommended guidelines on digital monitoring in order to respond in an appropriate way.



It explains what digital 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 digital 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) 800 047 8191

Email: enquiries@smoothwall.com

Web: www.smoothwall.com/contact

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 child-on-child 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 and 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. According to NHS England, 1 in 5 young people had a probable mental disorder in 2023.

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

Digital monitoring continues to be a key requirement in Keeping Children Safe in Education (KCSIE) 2025. Governing bodies and proprietors are tasked with ensuring that their school has “appropriate filtering and monitoring systems in place and regularly review their effectiveness.”

It states that monitoring systems are there to safeguard students and the responsibility should lie with the Senior Leadership Team (SLT), Governors and the Designated Safeguarding Lead (DSL).

Despite this, many schools are still unclear about how to safeguard vulnerable young people through digital monitoring and the role it plays in their safeguarding strategies.

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

A black and white photograph of a young boy with dark, wavy hair, looking down at a smartphone he is holding in his hands. The background is blurred, showing what appears to be a window with a grid pattern. The lighting is soft, coming from the side.

//
44.6% of young people
who reported having
a concern about their
mental health did not
seek help or advice.”

NHS Digital 2023

2.0 Guidelines and Legislation

In this section we review the main legislative and guideline changes and the provisions schools must evidence in relation to monitoring.

KCSIE 2025

- Schools in England are obliged to “ensure that appropriate filtering and monitoring systems in place.”
- Monitoring systems are there to safeguard children and the responsibility should lie with the Senior Leadership Team (SLT)/Governors and Designated Safeguarding Lead (DSL).
- School DSLs have a responsibility to understand the filtering and monitoring systems and processes in place as part of their remit.
- It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate students and staff.
- 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 MAT are expected to have their own individual policy.
- Schools should carefully consider how smart mobile technology is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.
- The child protection policy should also include how it approaches appropriate filtering and monitoring on school devices and school networks.
- 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.
- Safeguarding is defined as: “Providing help and support to meet the needs of children as soon as problems emerge.”
- All staff within schools should be aware of indicators of abuse, neglect and exploitation, understanding that children can be at risk of harm inside and outside of school and online.
- School staff should be aware that abuse, neglect, exploitation and other safeguarding issues are rarely standalone events and cannot be covered by one definition or one label alone. In most cases multiple issues will overlap one another.
- Children with special educational needs or disabilities (SEND), or certain medical or physical health conditions can face additional safeguarding challenges both online and offline. Governing bodies should ensure their child protection policy reflects the fact that additional barriers can exist when recognising abuse, neglect and exploitation in this group of children.
- 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.

Filtering and Monitoring Standards for Schools and Colleges

The Department for Education (DfE) outlines 3 standards schools should already be meeting with their monitoring provision(s):

- Schools should identify and assign roles and responsibilities to manage monitoring systems - governing bodies and proprietors have overall strategic responsibility.
- Schools should review their monitoring provision(s) at least annually.
- Schools should have effective monitoring strategies in place that meet their specific safeguarding needs.

Working Together to Safeguard Children 2023

- Communication between institutions and multi-agency safeguarding partners is vital to be able to identify and respond to the needs of children and young people.
- Safeguarding and child protection measures must address risks that occur outside the home, including online.
- 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 should understand their role in identifying emerging problems and effective sharing of information is essential for early identification of need, assessment, and service provision to keep children safe.
- School leaders should use evidence from direct practice in their area to evaluate what is and isn't working for the children in their care. Effective collection, sharing and analysis of data, enables staff to identify potential safeguarding risks and emerging trends.
- Schools should consider the influence of harmful groups or individuals that operate online and identify patterns of harm and risk in this context.
- Clear evidence will help the agencies to gain a full picture and put the right measures in place. It also aids them in identifying patterns of behaviour that may indicate that a child is at risk of going missing.
- DSLs and headteachers should ensure that children receive the holistic support they need, and support other staff in identifying issues such as discrimination, disparity, and negative stereotypes.
- Schools should provide effective support as soon as a problem emerges to avoid escalation.



The Data Protection Act (DPA) and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children.”



OFSTED

Schools also need to be aware of the increasing importance digital monitoring plays within OFSTED inspections, with guidance specifically provided to support inspectors when visiting schools/colleges.

- Inspectors should consider the extent to which schools understand the risks associated with using technology, including social media, bullying, grooming, exploitation, radicalisation or abuse of children or learners.
- Inspectors should consider the extent to which leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's wellbeing.
- Inspectors will look for evidence that leaders of early years settings implement the required policies on the safe use of mobile phones and cameras in settings.
- Inspectors should be able to see evidence of an effective whole school approach to safeguarding. This means ensuring that safeguarding and child protection are at the forefront of, and underpin all relevant aspects of, process and policy development. Ultimately, all systems, processes and policies should operate with the best interests of children and learners at their core.
- Inspectors should consider if there is a robust and proactive response from adults working with children and learners that reduces the risk of harm or actual harm to them. Adults working with them should know and understand the indicators that may suggest that a child, learner or vulnerable adult is suffering or is at risk of suffering abuse, neglect, exploitation or harm.
- Inspectors should consider the extent to which leaders and managers have put in place effective child protection and staff behaviour policies that are well understood by everyone in the setting. For schools and further education and skills settings, there are also effective policies for tackling bullying, sexual harassment, online sexual abuse, exploitation and sexual violence between children.
- Inspectors should examine how a school is implementing its safeguarding policies and processes effectively and how it keeps them under review.

The Prevent Duty 2023

Schools should be aware of the increased risk of online radicalisation, as terrorist organisations 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.

- “Settings should not only be alert to violent extremism but also non-violent extremism, including certain divisive or intolerant narratives which can reasonably be linked to terrorism.”
- “Each setting should perform a risk assessment which assesses how their learners or staff may be at risk of being radicalised into terrorism, including online. Where specific risks are identified, settings should develop an action plan to set out the steps they will take to mitigate the risk.”

The Children’s Act 1989 and 2004

Local authorities in England have overarching responsibility for safeguarding and promoting the welfare of children in their area. As part of this, they have a number of statutory functions under the 1989 and 2004 Children Acts, including undertaking assessments of children who are in need or are suffering, or likely to suffer, significant harm in order to determine what services should be provided and what action should be taken.

The Education Act 2002

Section 157 for academies and independent schools requires governing bodies of maintained schools and further education colleges to ensure they safeguard and promote the welfare of children for all pupils and students under the age of 18.

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.

Technology is a major force for good in learning. It is also a major risk factor for a number of issues concerning young people, not least of which are cyberbullying, sexual exploitation, radicalisation and the mental health factors and dangers to life that arise from these.

You must review whether your school is using the most effective solutions to identify your students in need.

UK Safer Internet Centre Appropriate Monitoring Guidance

This guidance highlights that schools should be led by their own risk assessments when deciding what level of monitoring is right for them. They must be satisfied that their monitoring strategy or system at least covers the following content:

Illegal online content

Child sexual abuse: Manipulative or coercive behaviour towards a child that promotes sexual abuse or exploitation of children. This is strictly prohibited and carries severe legal penalties.

Controlling/Coercive behaviour: Actions or content that involves psychological abuse, manipulation, or intimidation to control individuals (often occurring in domestic contexts).

Extreme sexual violence: Graphic depictions of acts of sexual violence, intended to shock or incite similar behaviour. It is illegal under UK law.

Extreme pornography: Pornographic material depicting acts that threaten a person's life or risk serious injury, and is deemed obscene and unlawful.

Fraud: Deceptive online practices designed to secure unfair or unlawful financial gain, e.g., phishing and scam activities.

Racially or religiously aggravated public order offences: Content inciting hatred or violence against individuals based on race or religion, undermining public safety.

Inciting violence: Online material encouraging or glorifying acts of violence, posing a risk to public safety and order.

Illegal immigration and people smuggling: Content promoting or facilitating unauthorized entry into a country, including services offering illegal transportation or documentation.

Promoting or facilitating suicide: Material encouraging or assisting individuals to commit suicide. It poses serious risks to vulnerable populations.

Intimate image abuse: The non-consensual sharing of sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.

Selling illegal drugs or weapons: Online activities advertising or selling prohibited substances or firearms, contravening legal regulations.

Sexual exploitation: Content that takes advantage of individuals sexually for personal gain or profit, e.g., trafficking and forced prostitution.

Terrorism: Material promoting, inciting or instructing terrorist activities, to radicalise individuals or coordinate acts of terror.

Primary Priority, Priority or inappropriate Content

Gambling: Content that enables gambling.

Harmful content: Content that is bullying, abusive or hateful. Content depicting or encouraging violence or injury. Content encouraging dangerous stunts and challenges, e.g., the ingestion of harmful substances.

Hate speech/Discrimination: Content expressing hate or encouraging violence towards a person/group based on something such as race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010.

Malware/Hacking: Promoting the compromising of systems including anonymous browsing and other filter bypass tools, as well as sites hosting malicious content, e.g., ransomware and viruses.

Mis/Dis Information: Promoting or spreading false or misleading information intended to deceive, manipulate, or harm, e.g., content undermining trust in factual information.

Pornography: Content that includes explicit imagery or sexual acts.

Self-harm and eating disorders: Content encouraging, promoting or offering instructions for self harm, eating disorders or suicide.

VAWG: Promoting or glorifying violence, abuse, coercion, or harmful stereotypes targeting women and girls, e.g., content that normalises genderbased violence.

3.0 The Digital Monitoring Challenges Schools Face

Schools are now under more pressure than ever to keep tabs on what pupils do, say and share on digital devices.

With class sizes often growing to more than 30 students, identifying every risk can feel like an impossible task, especially for a busy and overstretched school.

To add to the concern, new digital risks are emerging at the same time as teachers' workloads become increasingly unmanageable.

Serious Incidents

338 serious incidents reported to Ofsted in 2024/25

Source: Gov.uk

Online Grooming

82% rise in online grooming crimes in the last five years

Source: NSPCC 2023

Bullying

1 in 5 students experience at least one type of **online bullying behaviour**

Source: Crime Survey for England and Wales (CSEW) 2023

Social Media

4 out of 5 young people say social media platforms make their **feelings of anxiety worse**

Source: Royal Society for Public Health Report

Lack of Resource

41% of teachers say their **workload is unmanageable** all or most of the time

Source: National Education Union 2024

Sexual Abuse

More than **300 million** children a year are **victims of online sexual exploitation and abuse**

Source: Childlight Global Child Safety Institute, University of Edinburgh, 2024



In 2024, Smoothwall Monitor identified a child suspected to be at serious risk every 2 minutes.

Smoothwall Monitor Data



Schools can often be left in the dark

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 vice versa. From hurtful messages to sharing images, schools can struggle to keep up and are often in the dark about 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 a digital monitoring solution, schools are unlikely to meet their legal obligations or duty of care.

The long-term impact if risks are not identified

According to [Manchester University NHS Foundation Trust](#), 1 in 3 diagnosed mental health conditions in adults directly relate to adverse childhood experiences. Furthermore, around 50% of mental health conditions are established by the time a child reaches the age of 14, and 75% by age 24 ([Gov.uk](#)). Early intervention through digital monitoring can reduce this significantly.

The imperative for schools

Schools must review whether they are using the most effective solutions to identify students in need. Technology-based digital monitoring solutions enable schools to identify potential 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.

4.0 The Vital Role of Digital Monitoring

As online dangers continue to increase so does the technology capable of addressing them.

What is digital monitoring?

Digital monitoring is a technology system in which digital devices within a school are constantly monitored to check for signs of risk in children.



For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.”

The Department for Education

Helping identify risks

Digital monitoring helps you to identify students at potential risk quickly. Serious risks such as suicide, grooming, or gang meetings 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 or 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.

Digital 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 digital monitoring solution 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 on a digital device, a screen capture is made by the digital monitoring system. This capture could be of a browser, an email, a Microsoft document, a social media platform or a chatroom. Digital monitoring is not like CCTV that films everything. It only captures the 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, enabling you to see the details when you log in and decide which alerts may be false positives, and which may require immediate attention. 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 digital 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 remaining false positives.

Severe alerts are immediately communicated via phone call, and lesser alerts may be sent in conveniently timed reports. Most providers have a safeguarding portal where you can log in and see the full context of the alert and gather any extra evidence you may require.

Key differences



Non-third party moderated

- Lower cost
- Allows your school to create its 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 has more time to analyse and carry out risk assessments.

Third-party human moderated

- AI profiling creates a clear picture of the context of an alert, removing many false positives and therefore reducing DSL workload
- A human moderator - part of a team of experts - will check all of your school's captures and analyse their priority grade whilst removing any false positives that may have slipped through
- Works offline
- Is a more time efficient digital monitoring solution as most false positives will be removed

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

5.0 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' another pupil.
- 3. Later that afternoon, Bobby stabbed another pupil.
- 4. The log was found the next day by the school technician, after painstaking forensic analysis of the computer Bobby was using.

If digital 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.

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

Jessica year 11

Risk type:
Mental health

- 1. Jessica was working on a computer in the school library.
- 2. She typed "how to cope with depression and anxiety" into Google.
- 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.

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

Monitoring type: Non third-party moderated

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.

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:
Child-on-child 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.

The school added customisation around Sara Potts' 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.

Emily year 6

Risk type:
Vulnerable student - eating disorder

1. Emily was sitting at a school computer during her lunch break.
2. She opened an AI chatbot and pretended to be an overweight adult looking for quick weight loss tips. The chatbot offered her advice on how to limit calories and distract herself from thinking about food.
3. The searches for "rapid weight loss tips" triggered an alert.
4. The school DSL picked up the alert. She was able to intervene by asking Emily to come and talk to her.

The DSL was able to offer Emily a safe space where she could discuss her worries about her weight. Emily was referred to a therapist specialising in eating disorders. The digital monitoring system de-escalated the problem and ensured Emily received the help she needed.

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.

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 "can i cut my hair myself".
2. An alert was raised for self harm because of the word 'cut'.

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

6.0 Providing Evidence for Ofsted

Ofsted will ask your schools or institutions to provide evidence of **appropriate monitoring**.

A technology-based digital monitoring solution will help you and your school evidence appropriate monitoring 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 a comprehensive picture of the risk landscape affecting your school.
- Provide a full evidence-based picture of the safeguarding provision and communicate effectively to outside agencies to ensure those at risk are identified and receive support at the right time.
- Demonstrate far reaching effective arrangements to identify children at risk.

A high quality digital monitoring solution will expand your safeguarding provision whilst reducing the number of false positives, supporting and facilitating, not adding to, existing resource requirements. (A human moderated monitoring solution removes false positives almost entirely.).

The reality is your school will not meet your obligations if you remain unaware of troubled students or students at an early stage of 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 digital monitoring make this easier than ever before.



7.0 How to Ensure Your School is Monitoring Appropriately

There are steps every school can take to ensure they are monitoring appropriately.

1. Ask your school to review their current monitoring practices using the handy matrix below.
2. Assess areas of non or weak compliance to determine the required level of monitoring support.

1. Ask your school to review their current monitoring practices

You should encourage your school to review whether they are using the most effective solutions to identify students in need. The matrix on the next page shows government recommended guidelines together with a traffic light system to highlight where your school's monitoring gaps may be.

	Green	Amber	Red
Policy/set-up			
Monitoring policy	We use an acceptable use policy which is embedded into the culture of our school. We also use it for the purpose of teaching online safety.	We use one acceptable use policy with all students.	We tell students what they should and shouldn't do when accessing the Internet.
Devices	Our system monitors all school devices.	Our system works on all managed devices in schools.	Our system only works on desktop computers / we only use physical monitoring.
Multi-Academy Settings	Our system is fully customisable with a granular configuration that gives access to a full overview of all schools and a singular view for individual schools. And / or we use a human moderator with a singular portal for individual schools to access.	We monitor an overview system but it is not possible for individual schools to see a portal of monitored activity relevant to their individual school.	A granular view is not possible. We need a separate system for each individual school.
Processes			
Prioritisation alert management	Alerts work in real-time and let the DSL react to concerns when needed immediately. They are activated by various sources online and offline.	Alerts are risk-graded but do not show in real-time. Alerts may not occur out of browser. The system may be limited in the way it makes captures.	The DSL must look through a logbook for any issues. There is limited or no prioritisation. We have limited categorisation. A teacher makes a note if they see an incident.
Flexibility	We use intelligent analysis and profiling to gain a full picture of a student's activity. We used added human moderation to 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. We only use physical monitoring.
Procedures			
Reporting and evidence	We can view a full contextual background in a report. We can analyse peer trends and pupil profiles.	Context is given with screenshots as evidence.	Logbooks take much time in making sure nothing is missed. Limited evidence is given. We have no context. The tutor reports incidents to DSL to note down.
Data storage	We hold data in a guarded off-site setting with robust levels of online protection.	We hold data in a secure setting with good online protection.	We hold data physically on site and have no extra security.

	Green	Amber	Red
Impact			
What is the outcome and impact of your monitoring strategy?	Our 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.	Our alerts are listed in risk order. This relies on the DSL checking through alerts. Gives text evidence.	We don't act on alerts quickly enough. Evidence is very limited. Teachers may not see misuse or risks as children are good at concealing screens.
Suitable for			
Size of institution / staff / student ratio	Our monitoring provision is suitable for clusters of schools looking to have effective granular controls over their monitoring arrangements.	Our monitoring provision is suitable for settings in which schools do not require their own access to evidence trends and are happy with reports created.	Our provision is not suitable for Multi-Academy Trusts.
Restrictions			
Any limitations	Not controlled completely within individual schools.	Will take more time in removing false positives and may not give enough evidence for disciplinarys.	We have hundreds of students. We manually check log files or watch over the shoulder of students. We don't always understand the logs.

2. Assess areas of non or weak compliance to determine level of monitoring support needed

The result of the review will determine your next step. If your school predominantly reports greens then your need for further action will be low. If your assessment reveals varying levels of provision you may consider recommending a technology-based monitoring solution.

If your assessment reports predominantly ambers or reds, you may wish to implement school-wide digital monitoring as a means of raising standards to a more appropriate level quickly.



A good digital monitoring solution will not invade privacy. It will pick up risk concerns that should be identified, as outlined by KCSIE guidelines.

8.0 Integrating Digital Monitoring into Your Safeguarding Strategy

It's important when implementing a digital 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 digital monitoring solution fit into your school's processes for identifying students at risk?
- Will it be easily accessible to the DSL, 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 your processes have flagged.
- Does the solution allow your school to react quickly to concerns? Ask how long it takes for an alert to take place and whether it functions in real-time.
- Does the solution have the right set-up for supporting multiple schools at once?
- Does it include online and offline captures for browsers, email, Microsoft documents and chat rooms? 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 school's ability to spot risks.
- Ensure your system monitors multiple languages if needed.

Integrating with your safeguarding policies

- Will the monitoring solution help 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 digital monitoring solution will not invade privacy. It will pick up risk concerns that should be identified, as outlined by KCSIE guidelines.
- Check that you are aware of how long data will be stored and whether it is kept in a secure setting.
- Ask where support and development for the solution will take place. Check it is within a country deemed to have adequate data protection.

Integrating with your safeguarding procedures

- Once a pupil at risk has been identified, check that your digital monitoring solution supports the procedures that follow.
- Does it provide evidence and details 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.

9.0 Frequently Asked Questions

How much should we expect to pay for digital monitoring?

Digital 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 vary 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 it at <https://smoothwall.com/how-to-create-a-case-for-funding>

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

Digital monitoring is not affected by the Data Protection Act and GDPR. KCSIE 2025 states:

“DPA and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children.”

How do we know that a digital 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 digital 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's network. Smoothwall's digital monitoring solution has no discernible impact on performance and works silently in the background. A user will not be aware that digital monitoring is taking place or that a capture has been taken.

What's involved in implementing a digital 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 straightforward, with no technical knowledge required.

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

Web filtering blocks content to prevent it being seen and accessed by students. It is essential. However, it cannot monitor what a child types into their device. Most web filtering systems do not send alerts in real-time, enabling you to act upon them quickly. Digital monitoring and web 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 school is overstretched as it is. Won't digital 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 digital monitoring make unnecessary captures of 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 digital monitoring system will vary and have flexible settings to suit your environment.

Is digital 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 digital 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 digital safeguarding experts. We'll be happy to help.

Tel: +44 (0) 800 047 8191

Email: enquiries@smoothwall.com



Appendices

Further reading

Digital 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>

Smoothwall Monitor Q&A

Produced by Smoothwall's digital safeguarding experts to help DSLs to better understand digital monitoring and decide whether it should be a part of their school safeguarding provision..

Available at: <https://smoothwall.com/digital-monitoring-for-dsls-your-key-questions-answered>

Smoothwall Monitor Solution Brochure

Learn about Smoothwall Monitor, our real-time, human-moderated digital monitoring solution

Available at: <https://smoothwall.com/solutions/monitor>

About Smoothwall

Smoothwall is part of Qoria, a global technology company dedicated to keeping children safe and well in their digital lives. Over 32,000 schools globally depend on our technologies to provide better student digital safety and wellbeing support.

From our humble beginnings in 2000 we have been dedicated to empowering educational organisations to digitally safeguard the young people in their care. Our solutions are innovative and pioneering and developed from the ground up to meet and exceed the legislative requirements set out by the Department for Education, as outlined in the Prevent duty and Keeping Children Safe in Education.

Digital safeguarding solutions were historically seen as security products to be selected, deployed and managed by a school/college's ICT department. And while the ownership remains generally true, the meteoric rise in the use of the internet as a vital tool for learning has firmly placed digital safeguarding on the agenda of most educational stakeholders.

Web filters today are not tools for blocking content. They are a means of improving learning outcomes by enabling students to freely access rich internet content, protected by granular filtering, controls and alerts to ensure any risks and safeguarding issues are quickly and accurately identified. Schools/colleges favour Smoothwall because of our understanding of this core concept and our pioneering solutions that support it.

Where Smoothwall Filter dynamically analyses content and intelligently blocks harmful content, Smoothwall Monitor is installed onto the school/college's computers where it analyses on-screen content and any keystrokes made.

Words or phrases indicating the user may be at risk of harming or being harmed are captured in a screenshot 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 do safeguarding issues such as mental health, cyberbullying, radicalisation and child sexual exploitation. The demands placed on the physical eyes and ears of teachers far exceed their ability to identify all but the most obvious risks, and puts the organisation at odds with both student needs and statutory guidelines.

Smoothwall's robust filtering and monitoring provision work in tandem to keep your young people safe and your organisation compliant with the legislation, guidelines and recommendations placed upon it.

Our partners

Smoothwall are members of the Internet Watch Foundation (IWF) and implement the Child Abuse Image Content list of domains and URLs. Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

Smoothwall partners with EduGeek and regularly consults IT leaders, DSLs, headteachers, teachers, and a range of supporting bodies across UK Education.

Contact us

Ask yourself

Are you confident that your school is monitoring effectively, keeping children safe in real-time, and fulfilling the requirements set out in KCSIE and Ofsted's inspection guidance?

If you don't know, it's time to check. If you're unsure or have a question, contact Smoothwall's digital safeguarding 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) 800 047 8191

**Email: enquiries@smoothwall.com
smoothwall.com**



smoothwall® by Qoria

Smoothwall is the leading provider of digital safeguarding solutions in UK education. For more information, visit our website or get in touch with our team of experts.

Web: www.smoothwall.com

Tel: +44 (0)800 047 8191

Email: enquiries@smoothwall.com

Qoria

Smoothwall is part of Qoria, a global technology company, dedicated to keeping children safe and well in their digital lives. We harness the power of connection to close the gaps that children fall through, and to seamlessly support them on all sides - at school, at home and everywhere in between.

Find out more
www.qoria.com