Smoothwall for Education

Whitepaper

Digital Safeguarding

A Complete Guide to Active Monitoring for Colleges

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

smoothwall®

smoothwall.com

Contents

Appendices

About this document

This document has been produced to help FE colleges navigate the legislation and recommended guidelines on active monitoring in order to respond in an appropriate way.

Written by Smoothwall's Online Safety Experts, it explains what monitoring is, why it's needed and how you can integrate it into your existing safeguarding strategy.

Essential reading for: Designated Safeguarding Leads, Heads/Principals, Governors, Proprietors, and anyone interested in or responsible for ensuring safeguarding compliance within a college.

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

1.0 Introduction

The Internet, computers and mobile devices are all a normal part of life for most young people.

Many will already own multiple connected devices and for colleges, the Internet and computers are an essential component for studying.

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

Bullying within colleges is nothing new, but cyberbullying, peer on peer abuse and harassment has become a rising concern. Where previous generations of young people could go home to safety, the viral nature of their online life means they no longer have a safe place to go to. They have no escape.

Young people can be on the receiving end of humiliating or degrading messages, sexual images or videos 24/7. With this age group, a vulnerable one in society, young people can be exposed to a whole raft of dangers and negative influences, including sexual exploitation, radicalisation and gender-based violence.

The impact of this can be seen by a surge in the number of young people suffering from mental health issues as a result of their online activities. An AOC study of FE colleges found that 69% had seen a significant rise in mental health issues in 16-18 year olds over the past 3 years.

Young people's online safety 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 and colleges, 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 colleges need to ensure *"appropriate filters and… monitoring systems are in place"*.

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

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

> 69% of FE colleges have seen a significant rise in mental health issues in 16-18 year olds over the past 3 years.

Association of Colleges, 2017.

2.0 Changes to Monitoring Guidelines and Legislation

As we know there are a number of legislative and statutory guidelines, including several recent and important changes, that necessitate some form of monitoring within your college. Below is a summary.

The Education Act 2002

Section 175 of the Education Act 2002 requires governing bodies of maintained schools and further education colleges (including sixth form colleges) to ensure they safeguard and promote the welfare of children for all pupils and students under the age of 18.

The statutory guidance KCSIE gives specific guidelines for schools and colleges, and Working Together to Safeguard Children details how schools and colleges should work with health provisions, social care, the Police, and other services to promote the welfare of children and protect them from harm.

KCSIE 2018

- 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 college 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 college.
- Colleges 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.
- Assessments of children should consider whether wider environmental factors are present in their life that are a threat to their safety and/or welfare.
- DSLs will likely have a "complete safeguarding picture".
- The DSL should take lead responsibility for safeguarding and protecting young people, including online safety.
- DSLs must be up to date in training for online safety.
- DSLs must understand the vulnerability of children with SEN and disabilities in the online environment – with everything from online bullying, to grooming to 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 young people safe whilst they are online at college.
- Data protection and GDPR should not interfere with the ability to share information relating to safeguarding.

Working Together to Safeguard Children 2018

- Communication between institutions and multi-agency safeguarding partners is crucial (ages up to 18).

- Clear evidence and a full picture will help the agencies put the right measures in place.

- Colleges 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 young people 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 college is safeguarding young people appropriately in the online environment.

- Colleges understand the risks posed by adults or learners who use technology, including the Internet, to bully, radicalise or abuse young people or other learners.

- There should be well-developed strategies in place to keep young people 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 young people and learners who may need early help or who are at risk.

- At all times colleges should be actively considering the risks posed to all their students and putting adequate measures in place to protect them and keep them safe.

The Prevent Duty 2015

It is essential that colleges remain fully aware of their legal obligation to fulfil the Prevent duty. The majority of extremist activity occurs through technology which is why it is important for colleges to robustly monitor for this kind of content.

Section 26(1) of the Counter-Terrorism and Security Act 2015 (“the Act”) imposes a duty on “specified authorities”, when exercising their functions, to have due regard to the need to prevent people from being drawn into terrorism. There is an important role for further education institutions, including sixth form colleges and independent training providers, in helping prevent people being drawn into terrorism. This includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. It is a condition of funding that all further education and independent training providers must comply with relevant legislation and any statutory responsibilities associated with the delivery of education and safeguarding of learners.

The UK Safer Internet Centre

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

- **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.

KCSIE, Working Together to Safeguard Children and Ofsted's inspection guidance all emphasise the need to pro-actively 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 college is using the most effective solutions to identify your students in need.

3.0 Meeting the Guidelines and Legislation

The challenges for colleges

Colleges are now under more pressure than ever to be able to identify any students at risk and any incidents happening within their organisations.

DSLs must ensure their college not only stays abreast of requirements, from both KCSIE and Ofsted, but that they execute the appropriate safeguarding measures correctly and timely.

With contact teaching hours largely varying and conflicting demands on a tutor's time and attention, identifying all safeguarding risks whilst still focusing on teaching can be an impossible task.

For example, a teenager might type a note to a friend to say he has a knife, and then quickly delete it. Or a registered sex offender may search for inappropriate content in their browser. A busy tutor is unlikely to see actions such as these.

In fact, these examples are both real life stories that occurred within a college setting and which were unseen by staff but detected by active monitoring within minutes. Staff were notified and able to respond appropriately. In the latter case, the individual was removed from the premises by Police within 45 minutes of typing the indecent content.

In these circumstances and many more like them, active monitoring prevented potentially dangerous situations arising.

Self harm

The number of girls under 18 being treated for **self-harm** in hospitals has **doubled** since 1997

Source: NHS Digital

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

Causes of criminality

1 in **4** people in young offender institutions reported **emotional** or **mental health** problems

Source: HM Inspectorate of Prisons

Cyberbullying

Half of all UK 16-18 year olds know a victim of **cyberbullying**

Source: Kids Insights

Bullying

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

Source: Annual Bullying Survey

Mental health

1 in **10** young people have a diagnosable mental illness

Source: Mental Health Foundation

Colleges 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-persistent consciousness in their lives. A constant obsession to obtain online personas 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 a college may impact on the environment inside the college and vice versa. From hurtful messages to sharing images, colleges 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 colleges to always have a "it could happen here" approach.

It is a particularly vulnerable time when students start college. They have a new-found independence and are enjoying new experiences as they develop into young adults.

For some students, it's a time when they may disregard their previous online safety advice and start to have an 'it won't happen to me' mentality. Serious risks are often shared online, whether it be a student with a knife, a student who is hours from suicide, or a student about to engage in illegal drug use, sometimes the only hint of this happening maybe through their use of technology.

With high risk comes the need to detect and react fast, and without an active monitoring solution, colleges 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 24, 75% of mental health issues will have already become established. Early intervention through appropriate monitoring can reduce this significantly.

The imperative for colleges

Statutory guidelines clearly put the onus onto colleges and safeguarding partners to act in a more preventative way and to increase measures to protect the most vulnerable of students.

Alongside this legislation, the Government's Transforming Children and Young People's Mental Health Provision green paper, shifts much of the responsibility for tackling mental health issues onto educational institutions.

The reality is your college will not meet its obligations while ever it remains unaware of troubled students or students at an early stage risk.

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

4.0 The Role of Monitoring

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

What is Monitoring?

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

Helping identify risks

Active monitoring helps to identify students at risk quickly. Serious risks such as a suicide, sexual abuse or a gang meeting can all be picked up in real-time if a user has used their keyboard 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 tutors who, in a busy teaching environment, may be unable to see what is happening online.

How it works

There are generally two types of active 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 active monitoring system. This capture could be in 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. Colleges 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 which alerts need 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 young person 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 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 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 communicated via phone call, 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.

Key differences

Non third-party moderated

- More affordable.
- Allows your college 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: Colleges 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 college'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: Colleges 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

Illustrative 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**

Henry year 12

Risk type:
Violence to others

1. Henry brought a knife into school.

2. He messaged one of his peers that he was going 'to get' another student.

3. Later that afternoon, Henry stabbed another pupil.

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

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

Stephanie year 13

Risk type:
Drugs

1. Stephanie was working on a shared document with a course friend.

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

3. At break-time, Stephanie and her class 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 12

Risk type:
Mental health

1. Jessica was in the college library working on a computer.

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 course friend noticed the scars that her DSL was informed.

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

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

Tamara year 12

Risk type:
Child exploitation - vulnerable student

1. Tamara was at a college computer.

2. She was sent a threatening email saying that if she didn't meet someone called Richard after college, 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 DSL picked up the alert and invited Tamara for a confidential chat.

5. After receiving information from Tamara, Richard was reported to the police and the college was able to give clear evidence of the incident. The monitoring system de-escalated the problem and ensured Tamara received the support she needed.

Matthew year 12

Risk type:
Violence

1. Matthew was in the college library working on a computer.

2. A class friend came in and wrote a note on the screen, "I think James brought in a knife".

3. Matthew read the note and quickly deleted it, meanwhile an alert was triggered at this point and sent to the college's DSL.

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

Sarah year 13

Risk type:
Cyberbullying

1. A relationship rift had caused a group of girls to target Sarah with anonymous and malicious messages online.

2. Disturbed by the cruel comments, Sarah told a tutor but didn't know who was responsible for doing it.

3. Using the monitoring portal, the DSL created a custom search using Sarah's name. The DSL received alerts of 3 girls sending the abuse within 24 hours and could follow up on the situation.

Monitoring type: **Third-party moderated**

Nadia year 13

Risk type:
Discrimination

1. Whilst writing a piece of coursework Nadia received racial and abusive messages on Facebook messenger.

2. Although Nadia ignored the messages, an alert was sent to the human moderator.

3. The human moderator could see how the messages displayed inappropriate language and notified the DSL.

4. The DSL logged into the monitoring console to see the full conversation and gain context of the situation.

5. The DSL was able to immediately intervene and implement the safeguarding policy for unacceptable behaviour.

Joey year 12

Risk type:
Suicidal

1. Joey 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 Joey had previously looked up paracetamol and Codeine. They contacted the college DSL immediately.

4. The safeguarding lead logged into the console, saw where in the college Joey was located, and put together a swift plan to intervene and implement the safeguarding policy for a young person at risk.

Tom year 12

Risk type:
Self harm

1. Tom was in a study group when he messaged a class friend on Facebook messenger and said "I'm going to kill you off on FIFA".

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

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 will ask your college to provide evidence of appropriate monitoring. A technology based active monitoring solution will help your college 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 college.
- Demonstrate far reaching effective arrangements to identify vulnerable people at risk.
- 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 the right support at the right time.

A high quality monitoring solution will expand your college's 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.)

The traffic light matrix below will help you evaluate your current monitoring provision against recommended guidelines.

Evaluating your existing monitoring system

	Green	Amber	Red
Policy/set-up			
Monitoring policy	We use an acceptable use policy which is embedded into the culture of our college. 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 college devices.	Our system works on all managed devices in college.	Our system only works on desktop computers / we only use physical monitoring.
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 tutor makes a note if they see an incident.

	Green	Amber	Red
Processes			
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.	We can customise their risk-grading and words to fit the cohort. We 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 student 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.
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	We hold data in a guarded off-site setting with robust levels of online protection.	We hold data is in a secure setting with good online protection.	We hold data physically on site and have no extra security.
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. Tutors 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 colleges looking to have effective granular controls over their monitoring arrangements.	Our monitoring provision is suitable for colleges who do not require their own access to evidence trends and are happy with reports created.	Large amounts of data created. Likely to need full time staff to monitor it. Risks could be missed.
Restrictions			
Any limitations	May have less customisation options. Not completely controlled within college.	Will take more time in removing false positives and may not give enough evidence for disciplinaries.	With most colleges holding 1000's of students, checking that no log is missed will take a huge amount of staff time.

5.0 Integrating Active Monitoring into Your Safeguarding Strategy

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

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 young person's safety.

The following key points should be considered in order to choose the right solution and ensure a smooth integration.

Integrating with your safeguarding processes

- Will the monitoring solution fit into your college'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 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 and whether it functions in real-time.
- Does it include online and offline captures for browsers, email, Microsoft documents or 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 college's ability to spot risks.

Integrating with your safeguarding policies

- 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 college 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 college?
- Check that you are aware of how long your data will be stored and whether it is kept in a secure setting.

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.

6.0 Frequently Asked Questions

How much should we expect to pay for monitoring?

Monitoring solutions range in price depending on the number of pupils, the quality and range of monitoring, whether it is real-time risk grading, whether it is 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 colleges budgeting for this?

Sources of budget vary from college to college. Since the DSL has lead responsibility for online safety under their college safeguarding remit, some colleges may choose to fund it from their risk / safeguarding budget whereas others might use their general or ICT fund. If this is a new addition, 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 college's 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 is a top priority and it is stored in a secure Microsoft Azure protected cloud data site.

How can we check the impact a monitoring solution might have on our 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 college network. All the Smoothwall monitoring solutions have no impact on performance and work silently in the background. A user will not be aware 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 or 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 give you a robust digital safeguarding capability that helps keeps you Ofsted compliant and your students safe.

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

Colleges are obliged to have appropriate monitoring in place. We recognise this is difficult to do with many monitoring systems due to the extra workload they create. At Smoothwall we offer a range of solutions that vary from using effective 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 still be there. Every college has different needs which is why Smoothwall monitoring systems are varied 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 time-frame 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

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 college 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®