Appropriate Monitoring for Schools

~~May~~ ~~xxx~~ 2026~~5~~

Schools[1] (and registered childcare providers) in England and Wales are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[2]. Furthermore, it expects that they "*assess the risk of* [their] *children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".* There are a number of self review systems (eg 360 degree safe[3]) that will support a school in assessing their wider online safety policy and practice. The Department for Education's statutory guidance 'Keeping Children Safe in Education'[4] obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks*[5]*from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

To further support schools and colleges in England to meet digital and technology standards, the Department for Education published Filtering and Monitoring Standards[6] in March 2023 (as part of a broader suite of educational technology standards and guidance[7]). In addition to aspects of both filtering and monitoring systems, these standards detail the allocation of roles and responsibilities, and that schools and colleges should be checking their filtering and monitoring provision at least annually. These standards were included within Keeping Children Safe in Education in 2023

Given the extent of personal data involved with some monitoring solutions, Schools and Colleges should consider undertaking a data protection impact assessment[8] and ensure that the adopted monitoring strategy is integrated within organisational policies and alongside relevant data sharing agreements.

The aim of this document is to help schools (and providers) comprehend, in conjunction with their completed risk assessment, what should be considered as 'appropriate' monitoring.

Monitoring Strategies

There are a range of monitoring strategies and systems, however the appropriate monitoring strategy selected should be informed by your risk assessment and circumstances. It is also vitally

[11] The schools and registered childcare settings specified in Schedule 6 of the Counter-Terrorism and Security Act 2015 (CTSA 2015)
[2] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/publications/prevent-duty-guidance
[3] http://www.360safe.org.uk/, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/
[4] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[5] Keeping Children Safe in Education Paragraph 136, Page 35 – Content, Contact, Conduct, Commerce
[6] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
[7] Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)
[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

important to review and refine the relevant policies as part of assessing (or implementing) a monitoring strategy or system. The following are examples.

1) Physical Monitoring

Physical monitoring can contribute where circumstances and the risk assessment suggests low risk, with staff directly supervising children on a one to one ratio whilst using technology. This could be: physical supervision of children whilst using the Internet or assigning additional classroom support staff to monitor screen activity;. The following are possible limitations or points to consider

- It is difficult to physically monitor any independent use of technology
- Can be resource intensive
- Less effective across a larger group or a group using mobile devices
- Students often adapt screen behaviour to avoid monitoring
- Advantage of immediate intervention when an issue arises which can be developed as a teaching opportunity

Regardless of monitoring strategy, physical monitoring may be required for devices or technologies that are not able to be monitored using other strategies, for example images or videos taken on mobile devices or cloud storage

2) Internet and web access

Some Internet Service Providers or filtering providers provide logfile information that details and attributes websites access and search term usage against individuals[9]. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches. The following are possible limitations or points to consider

- Assign appropriate responsibility for analysing the logfile information with sufficient capacity. These reports can often be difficult to understand and may require time and specialist technical and/or safeguarding knowledge to analyse.
- The frequency that block or monitoring lists are updated by your provider
- The logfile information should be able to identify an individual user (or group as appropriate) for effective intervention
- Logs need to be regularly reviewed, interpreted and alerts prioritised for intervention
- Information held by the school that indicates potential harm, must be acted upon
- Be aware of any limitations of the logfile information. Schools should ensure clear and appropriate data retention policies and logfiles (Internet history) should include the identification of individuals and the duration to which all data is retained.

3) Active/Pro-active technology monitoring services

Where the risk is assessed as higher, Active or Pro-active monitoring technologies may be suitable. These specialist services provide technology based monitoring systems that actively monitor use through keywords and other indicators across devices[10]. These can prove particularly effective in drawing attention to concerning behaviours, communications or access. These systems can take the form of:

[9] http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-for-education-settings

[10] Worth noting which devices and operating systems are covered (eg Windows, MacOS, IOS, Android)

Active monitoring where a system generates alerts for the school to act upon. Active Monitoring is most effective where:

- There is sufficient internal capability and capacity to interrogate and interpret the volumes of information and alerts generated by the system
- Appropriate Safeguarding expertise is assigned to review, prioritize and take action on alerts that signal potential harm.

Pro-active monitoring where alerts are managed or supported by a specialist third-party provider and may offer support with intervention. Proactive monitoring is most effective where

- School safeguarding staff are actively and immediately alerted to genuine risk of threats to health or life
- The provided SLA meets the school requirements
- Specialist organisations provide additional capability and capacity to support school safeguarding staff
- High number of devices are operating

Schools should understand how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Monitoring Content

Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system (including keywords if using technical monitoring services) at least covers the following content

Illegal Online Content	
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.

selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.

Primary Priority, Priority or inappropriate Content	Explanatory notes – Content or communications that
Gambling	Enables gambling
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or 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	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions
Pornography	displays sexual acts or explicit images and text
Self-Harm and eating disorders	encourages, promotes, or provides instructions for self harm, eating disorders or suicide
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.

Monitoring Strategy/System Features

Schools should consider how their system integrates within their policies[11] and should satisfy themselves the extent that their monitoring strategy meets the following principles

- Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access
- Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.
- BYOD (Bring Your Own Device) – if adopted by the school and the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), ensure it is deployed in accordance with policy and how data is managed. Does it monitor beyond the school hours and location? Be aware of the considerable privacy concerns related to this aspect.

[11] Example template policies can be found at http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

- Data retention – should be clear what data is stored, where it is stored (physically – ie cloud/school infrastructure) and for how long. This should also include any data backup provision
- Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers
- Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy.
- Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).
- Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the application of appropriate configurations for individual users.
- Impact - How do monitoring results inform your policy and practice?
- Monitoring Policy – How are all users made aware that their online access is being monitored? How are expectations of appropriate use communicated and agreed? Does the technology provider offer any advice or guidance?
- Mobile and app content – Mobile and app content is often delivered through different mechanisms from that delivered through a traditional web browser, including embedded browsers within apps and in app link handling. Schools and colleges should understand to what extent the monitoring system operates across mobile devices and app content, including whether it can inspect or report on activity occurring within apps (not only within an internet browser). Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this. ~~mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the monitoring system operate across mobile devices and app content. Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this.~~
- Multiple language support – the ability for the system to manage relevant languages to your school
- Prioritisation – How alerts generated via monitoring are prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?
- Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users. Monitoring should focus on school-owned and managed devices. When shared devices are used, schools should ensure users log in individually. This allows monitoring systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.
- Reporting – how alerts are recorded, communicated and escalated?
- Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity

Monitoring systems require capable and competent staff with sufficient capacity to effectively manage them, together with the support and knowledge of the entire staff. Monitoring systems are there to support the effective safeguarding of children and the responsibility should therefore lie

Commented [A1]: What has changed
- The wording has been clarified to reflect how monitoring operates across mobile devices and applications, not only within traditional web browsers.
- Reference has been added to in-app activity and embedded browsers, recognising that content may be accessed or displayed within apps rather than through a standalone browser.
- The expectation that providers clearly explain monitoring capability and configuration requirements for mobile and app content has been reinforced.

Why this change was made
- To reflect current patterns of device and app usage in education settings.
- To address safeguarding risks arising from app-based content delivery that may not be visible through browser-only monitoring.
- To support schools and colleges in understanding the practical coverage and limitations of monitoring on mobile devices.

with the school leadership/governors and Designated Safeguarding Lead as part of the establishment's broader safeguarding approach. Schools and Colleges should ensure that their staff, and in particular those responsible for and managing their monitoring strategy, have sufficient capacity and capability. Schools and Colleges should have policies and processes to support those staff responsible for managing monitoring systems. The UK Safer Internet Centre Helpline[12] may be a source of support for schools looking for further advice in this regard.

Filtering and monitoring systems are only ever tools in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum"*[13]. To assist schools and colleges in shaping an effective curriculum, UK Safer Internet Centre published ProjectEVOLVE[14]

Risk Assessment

UK Safer Internet Centre recommends that those responsible for Schools and Colleges undertake (and document) an annual online safety risk assessment at least annually or whenever any changes substantive occur, assessing their online safety provision that would include monitoring provision. The risk assessment should consider the risks that both children and staff may encounter online, together with associated mitigating actions and activities.

A risk assessment module has been integrated in *360 degree safe*[15]. Here schools can consider identify and record the risks posed by technology and the internet to their school, children, staff and parents.

Checks and Documentation

Schools and Colleges should regularly check that their filtering and monitoring systems are effective and applied to all devices. Checks should be conducted when significant changes take place (for example, technology, policy or legislation), in response to incidents and at least annually. These checks should be recorded, including details about the location, device and user alongside the result and any associated action.

Monitoring on Mobile devices

Schools and colleges should satisfy themselves that monitoring systems are correctly working across all their devices' and across all internet connections, including their mobile devices. If your school owns mobile devices such as iPads or other tablets as part of your teaching strategy, then consider the following practices to ensure monitoring is in place (you may need the help of your ICT support to do this):

For schools and colleges in England, the following DfE guidance is relevant

- Digital leadership and governance standards - Guidance - GOV.UK (www.gov.uk) – specifically guidance related asset registers in context of points 1 and 2 below
- Laptop, desktop and tablet standards - Guidance - GOV.UK (www.gov.uk)

[12] https://www.saferinternet.org.uk/helpline
[13] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[14] ProjectEVOLVE - Education for a Connected World Resources (https://projectevolve.co.uk/)
[15] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/

- Mobile phones in schools - GOV.UK (www.gov.uk)

:

1. Audit the mobile device estate by detailing all the mobile devices they have.
2. Understand and detail the applications (apps) they use and how these are managed (installed and deleted). Specifically, ensure that apps can be centrally, and routinely, removed from mobile devices. This is best achieved through the use of a Mobile Device Management (MDM). Where apps include embedded browsers or open links in other apps, schools and colleges should confirm whether monitoring (and reporting) applies to that activity~~Understand and detail the applications (apps) they use and how these are managed (installed and deleted). Specifically, ensure that apps can be centrally, and routinely, removed from mobile devices. This is best achieved through the use of a Mobile Device Management (MDM)~~.
3. Identify who is responsible for mobile devices as well as filtering and monitoring systems at the school, ensuring that the DSL is also aware (if different).
4. ~~3.~~
5. ~~4.~~ Test to provide confidence that the school's filtering and monitoring solution is working across all mobile devices, across installed apps (not just internet browsers) and in various physical locations. Schools can use testfiltering.com to help observe filtering behaviour on their connection, including where additional configuration (for example managed devices, certificates, or managed browsers) is required for particular tests. ~~Test to provide confidence that the schools filtering and monitoring solution is working across all mobile devices, across installed apps (not just internet browsers) and in various physical locations. Schools can use testfiltering.com to help in this regard.~~
6. ~~4.~~
7. Identify any vulnerable users of mobile devices, paying particular attention to ensure harmful content is not accessible on specific devices

Commented [A2]: What has changed
- The guidance on app management has been extended to include confirmation of whether monitoring applies to activity occurring within apps, including where apps use embedded browsers or open links in other applications.
- The section on testing has been clarified to explain that testing may require specific configurations, such as managed devices or certificates, depending on the monitoring and filtering approach in use.

Why this change was made
- To improve clarity about how monitoring operates in app-based environments.
- To ensure schools and colleges can accurately assess whether monitoring coverage extends beyond internet browsers.
- To support informed and realistic testing of monitoring and filtering arrangements across different devices and configurations.

Generative AI Technologies

New technology is enabling users to generate personalised content in real-time based on prompts and schools are being encouraged to exploit these potential advantages for "faster planning and record-keeping"[16]. The real-time nature and proliferation of these system present a challenge to schools when it comes to monitoring this type of content. Monitoring systems should maintain robust activity logging procedures which captures content created by Generative AI tools. Schools should reflect on the following, as part of any risk assessment, when considering their systems and deciding what generative AI systems they allow students and staff to use:

- The level to which your monitoring system can monitor content in real-time
- Assessing which generative AI systems the school which to approve for use after assessing safety features, and data protection
- Developing a policy around the use of generative AI systems
- Assessment of your ability to generate reports on the usage or generative AI systems within school

[16] Artificial Intelligence: Plan to 'unleash AI' across UK revealed - BBC News

Further Governmental considerations for adopting Generative AI technologies in schools:

- England – Generative artificial intelligence (AI) in education - GOV.UK (Jan 2025)
- Wales - Generative artificial intelligence in education - Hwb (Jan 2025)

This detail has been developed by the UK Safer Internet Centre, and in partnership and consultation with the 120 national '*360 degree safe Online Safety Mark*'[17] assessors and the NEN Safeguarding group (www.nen.gov.uk).

[17] www.360safe.org.uk, https://360safecymru.org.uk/, http://www.360safescotland.org.uk/