

Appropriate Monitoring for Schools

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”¹. 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 www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education published the revised statutory guidance ‘Keeping Children Safe in Education’² in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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.”

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

Physical Monitoring

Most suited where circumstances and the assessment suggests low risk, with staff directly supervising children whilst using technology. This could be: physical supervision of children whilst using the Internet; assigning additional classroom support staff to monitor screen activity; or actively monitoring all screen activity during a lesson from a central console using appropriate technology. The following are possible limitations or points to consider

- 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

Internet and web access

¹ Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance_England_Wales_V2-Interactive.pdf

² <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Some Internet Service Providers or filtering providers provide logfile information that details and attributes websites access and search term usage against individuals³. 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. These reports can often be difficult to understand and may require specialism 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

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 devices⁴. These can prove particularly effective in drawing attention to concerning behaviours, communications or access. These systems can take the form of:

- Active monitoring where a system generates alerts for the school to act upon
- Pro-active monitoring where alerts are managed by a third-party provider and may offer support with intervention.

The following are possible limitations or points to consider

- Can be expensive in terms of installing and maintaining technology
- Pro-active monitoring uses specialist organisations and may involve additional expense
- Active monitoring requires sufficient internal capability and capacity
- Active monitoring can initially generate significant volumes of information and alerts which can be difficult to interrogate and interpret.
- Assign appropriate Safeguarding expertise to review, prioritise and take action on alerts that signal potential harm

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

Content	Explanatory notes – Content or communications that
Illegal	Is illegal (eg. Child abuse images and terrorist content)
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.

³ <http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-for-education-settings>

⁴ Worth noting which devices and operating systems are covered (eg Windows, MacOS, IOS, Android)

Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance
Pornography	displays sexual acts or explicit images
Self Harm	promotes or displays deliberate self harm
Violence	Displays or promotes the use of physical force intended to hurt or kill
Suicide	Suggest the user is considering suicide

Monitoring Strategy/System Features

Schools should consider how their system integrates within their policies⁵ and should satisfy themselves that their monitoring strategy meets the following principles

- Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
- BYOD (Bring Your Own Device) – if 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
- Data retention – should be clear what data is stored, where and for how long
- Flexibility - changes in keywords (addition or subtraction) can be easily according to an agreed policy.
- 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?
- Multiple language support – the ability for the system to manage relevant languages
- 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?
- Reporting – how alerts are recorded, communicated and escalated?

Monitoring systems require capable and competent staff to sufficiently manage them, together with the support and knowledge of the entire staff. Monitoring systems are there to safeguard children and the responsibility therefore should lie with the school leadership/governors and Designated Safeguarding Lead

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”*⁶

⁵ Example template policies can be found at <http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy>

⁶ <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>