Filtering and monitoring - Essential information for Designated Safeguarding Leads

Key information from the session

Filtering:

- Who is your filtering provider?
- What filtering product do they provide?
- Is your filtering provider signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and a member of the Internet Watch Foundation?
- Do you have safe search enforced?
- Is safe search enforced on the network, devices or both?
- What search engine(s) is safe search enforced on?
- Do you have SSL inspection enabled?
- Can you set different filtering policies for specific users and user groups?
- How can temporary or permanent changes be made and who by?
- Are staff provided advice and access to release material, i.e., if the history teacher is covering WW2, can they access material on the Nazis without putting children at risk of radicalised material?
- Can you add your own keywords to the filter library that represent new concerns in your organisation?
- Are you confident that children can access support without unreasonably being blocked. For example, consider self-harm and anorexia.
- Does filtering work if devices are taken home?
- What traffic logs and analytics are provided?
- Does it provide any real-time alerts when a user's behaviour may be cause for concern?

Monitoring:

- Who is your provider? Do they offer a managed service or is it self–managed?
- Can you monitor **any device** that connects to the school network, including BYOD if applicable?
- What are the limitations of monitoring dependent upon device being used?
- Are set up requirements different dependent upon device being used?
- Does it capture only keyboard violations, or keyboard AND application/screen captures?
- Does it monitor activity when the device is offline?
- What library topics of concern are being monitored? Can you configure the library if required?
- What evidence is provided of the violation? Is it easy to understand and include useful information regarding the incident?

- Do you have access to a dashboard and reporting platform? Can you configure and customise reports and include email alert functionality to follow students at particular risk?
- Does it integrate with other safeguarding reporting tools e.g. CPOMS and MYCONCERN?
- Does it provide multi-language compatibility and local language, acronyms and algospeak?
- Does it have Active Directory synchronisation to identify individual user violations?

Filtering and monitoring systems should:

- be operational, up to date and applied to all:
    - users, including guest accounts?
    - school owned devices?
    - devices using the school broadband connection?
- allow you to identify:
    - device name or ID, IP address, and where possible, the individual?
    - the time and date of attempted access?
    - the search term or content being blocked?

Risk profiling:

- Have you carried out a risk profile that matches the needs of all learners and those considered to be vulnerable online?
- Has your organisation discussed what they consider to be problematic network behaviour that needs to be looked for when monitoring?
- Have 'at risk' individuals been identified and are proactively monitored?
- Do the filtering and monitoring systems work to support your identified risks to help protect your users?

DfE filtering and monitoring standards:

- A member of the senior leadership team and a governor, should be responsible for ensuring your filtering and monitoring standards are met.
- 4 standards to meet – 2 of the standards include a **review of systems** to be done at least annually, with evidence of the review being undertaken and a **review of the effectiveness of your systems.**
- Review filtering system requirements and monitoring strategies, drawing on policy documents, the risk profile of learners and the expectations included in these standards.