Lady Margaret School
Filtering and Monitoring Policy

Adopted: 7th November 2023
To be reviewed: November 2026

1. Introduction

Schools 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" (Revised Prevent Duty Guidance: for England and Wales, 2015).

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".

The use of technology has become a significant component of many safeguarding issues. With child sexual exploitation, radicalization and sexual predation, technology often provides the platform that facilitates harm. Our aim is to protect and educate the whole school community in our use of technology and to establish mechanisms to identify, intervene in and escalate any incident where appropriate.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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 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."

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

2. Aims

The school must ensure that it appropriately safeguards staff and students through an effective online filtering and monitoring regime.

3. Requirements of online Filtering and Monitoring

The school must ensure that internet systems are robust and appropriate for use by:

- Being able to demonstrate how its systems manage effective filtering and monitoring by the completion of an annual safety check, including filtering and monitoring (refer to Appendix A and B for supporting documentation).

- The completion of these checks will allow the school to construct a risk assessment that considers the risks that both students and staff may encounter online.

Actions To Take by the School	Actions to take by Governors
Recommendation that an online self-review takes place. For example: www.360safe.org.uk	Check that the school has completed annual Online Safety Checks (Filtering and Monitoring)
Complete the annual online filtering and monitoring checks	Check to see a risk assessment summary for students and staff is in place that satisfies the Prevent Duty
Complete a risk assessment that considers the outcomes of checks and limits the risks that students and staff may encounter online	

4. Roles and Responsibilities

The Governing Body

The Governing Body is responsible for monitoring the effectiveness of safeguarding within the school and making checks on the appropriateness of online filtering and monitoring systems.

The Governing Body will monitor the effectiveness of this policy and hold the headteacher to account for its implementation. They should be doing all that they reasonably can to limit students' exposure to online risks through the school's IT system.

Headteacher

The headteacher and appropriate senior leaders, are responsible for ensuring that this policy is adhered to, and that:

- The school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of students, and provide them with a safe environment in which to learn.
- They consider the age range of students, the number of students, how often they access the IT system and the proportionality of costs vs risks.
- Leaders conduct a risk assessment as required by the Prevent Duty.
- The school keeps a breast of statutory changes of government policy, and that the school meets all legal requirements for online monitoring and filtering.
- The school implements the relevant statutory arrangements for online monitoring and filtering.

Other staff

Other staff will ensure that they follow school policy with regard to appropriate use of the internet and that they use the school reporting mechanisms to alert leaders to any breaches in filtering and monitoring systems.

Links with other policies

This policy will be monitored and reviewed on a three-year cycle or as required by legislature changes.

This policy links to the following policies and procedures:

- Staff Code of Conduct
- Safeguarding and Child Protection Policy

Appendix A - Example Provider Checklist for Filtering

School	
Name and contact details of Network Manager	
Filtering System	
Date of assessment/checklist	

System rating response to use in the check boxes below:

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟧

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
● Are IWF members		
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content:

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	-promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		
Drugs / Substance abuse	-displays or promotes the illegal use of drugs or substances.		

Extremism	-promotes terrorism and terrorist ideologies, violence or intolerance.		
Malware / Hacking	-promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.		
Pornography	-displays sexual acts or explicit images.		
Piracy and copyright theft	-includes illegal provision of copyrighted material.		
Self-Harm	-promotes or displays deliberate self-harm (including suicide and eating disorders).		
Violence	-displays or promotes the use of physical force intended to hurt or kill.		

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other elements.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		

● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		
● Identification - the filtering system should have the ability to identify users		
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		
● Multiple language support – the ability for the system to manage relevant languages		
● Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices		
● Reporting mechanism – the ability to report inappropriate content for access or blocking		
● Reports – the system offers clear historical information on the websites visited by your users		

Filtering systems are only ever a tool 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"

Appendix B Example Provider Checklist for Monitoring

School	
Name and contact details of Network Manager	
Filtering System	
Date of assessment/checklist	

System rating response to use in the check boxes below:

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟧

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
● Are IWF members		
● Work with CTIRU ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’		

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	-is illegal, for example child abuse images and unlawful terrorist content.		
Bullying	-involves the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.		

Child Sexual Exploitation	-encourages the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.		
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.		
Suicide	-suggests the user is considering suicide.		
Violence	-displays or promotes the use of physical force intended to hurt or kill.		

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• 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 (i.e. not owned by the school), how this is deployed and supported and how data is		
managed. Does it monitor beyond the school hours and location		
• Data retention –what data is stored, where and for how long		
• 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 – schools ability to amend (add or remove) keywords easily		
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		
• Multiple language support – the ability for the system to manage relevant languages?		
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		
• Reporting – how alerts are recorded within the system?		

Please note below opportunities to support schools (and other settings) with their obligations around Keeping Children Safe in Education
