

# **ST ANDREW'S METHODIST PRIMARY SCHOOL**



## **Monitoring and Filtering Systems**

Reviewed January 2026  
Headteacher: Anne Barker

Designated Safeguarding Lead: Anne Barker

Named Governor for monitoring and filtering: Margaret Hughes

*Reviewed by the Staffing Committee of St Andrew's Methodist Primary School meeting  
February 2026*

Date of Next Review January 2027

This policy has been scrutinized to ensure it meets the requirements of the single equality duties. The school will make every reasonable adjustment to comply with the duties and actively avoid discrimination.

**Appropriate filtering and monitoring**

## **INTRODUCTION**

Schools need to do all that they reasonably can to limit children's exposure to risks from the school's IT system. Keeping Children Safe in Education (KCSIE) requires schools to ensure appropriate webfiltering and monitoring systems, which keep children safe online but does not "overblock". Filtering is a means of restricting access to harmful content."

Since KCSIE 2025, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead (DSL) now has lead responsibility for filtering and monitoring. At St Andrew's the DSL is the headteacher.

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

As schools get to grip with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Our safeguarding team will work closely with our MGL technical support staff for this to be possible, and technicians will be charged to carry out regular checks and feed back to the DSL.

### **ALL STAFF SHOULD:**

- Be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over-blocking.
- Have an understanding of the difference between filtering and monitoring and the meaning of overblocking.
- Submit concerns at any point via the CPOMS online recording system.
- Give feedback at the time of the regular checks, which will take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding briefings as well as via the acceptable use policy and regular training reminders in the light of the annual review and regular checks that will be carried out.

NB: 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.

At St Andrew's Methodist Primary School

- web filtering is provided by **Smoothwall** on school site and for school devices used in the home.
- changes can be made by the MGL technician on request and by the school business manager.
- overall responsibility is held by the headteacher, with further SLT support from the deputy headteacher and school business manager.
- Technical support and advice, setup and configuration are from MGL.
- Regular checks are made half termly by the DSL to ensure filtering is still active and functioning everywhere. Any identified concerns are evidenced in an online log eg. CPOMS.
- An annual review is carried out as part of the Salford safeguarding audit tool.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices.

At St Andrew's Methodist Primary School we use:

- physically monitoring by staff watching screens of users
- teaching pupils to report concerns regarding their own or other devices.
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services. This is Smoothwall which is monitored by a third-party service.

## **THE SMOOTHWALL FILTERING SYSTEM**

The Schools' Internet Service includes a managed firewall and Smoothwall web filtering service.

The Smoothwall filtering service is designed to facilitate the effective provisioning of safeguarding in a school environment and meets legal mandates set out under the Prevent Duty and Keeping Children Safe Online.

Smoothwall Filter is compliant with DfE Standards and KCSIE (Keeping Children Safe in Education) guidelines.

While centrally managed and updated, the service also enables school to block sites that is deemed inappropriate. Headteacher and Deputy will receive activity reports daily to their email.

Smoothwall Filter generates real-time alerts for incidents across seven category rule sets, ensuring prompt attention to potential risks. It also logs search behaviours by

individual users or groups, supporting incident investigations and helping inform digital safety education.

The 7 primary category rule sets are:

1. **Adult Content - Pornography:** Blocks access to explicit, pornographic, and, in some cases, sexualized, non-explicit websites.
2. **Abuse | Bullying | Suicide (Self Harm):** Identifies and restricts access to content related to self-harm, suicide, and cyberbullying to protect vulnerable users.
3. **Substance Abuse - Drugs/Alcohol/Tobacco:** Restricts content that promotes or facilitates the use of illegal drugs, prescription drug abuse, alcohol, or tobacco.
4. **Criminal Activity - Weapons/Violence:** Blocks content related to personal weapons, illegal acts, and violent, or graphic content.
5. **Radicalisation - Terrorism/Extremism:** Implements a specialized, "police-assessed list" of unlawful terrorist content, extremism, and radicalizing material.
6. **Intolerance - Hate Speech/Discrimination:** Blocks websites that promote prejudice, racial hatred, and discrimination against individuals or groups.
7. **Content Modification & Sensitive Content:** This category involves inspecting content for hidden risks—such as in HTTPS traffic—and managing content that, while not strictly illegal, is deemed inappropriate for the age group or context (e.g., specific social media or gaming).

## THE SCHOOL MONITORING SYSTEM

The DSL will monitor the filtering system by;

- Monitoring reports received daily, higher-level category sends a report immediately to headteacher and deputy.
- Review and extract reporting data
- Immediately responding to any email alerts
- Recording any identified alerts electronically eg; via CPOMS. MGL helpdesk

## SUMMARY

Filtering systems are only ever a tool in helping to safeguard children when online and we recognise our 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”.