



Web Filtering and Monitoring Statement 26/27

The school is committed to reviewing this policy regularly to ensure it remains compliant with current legislation, statutory guidance, and best practice.

School Name: The Kassia Academy

Address: Fallowfield Grove, Longbarn, Warrington, WA2 0QQ

Telephone: 01925 452010

This document is classified as a controlled document. Printed copies may not be the most up- to-date version. The latest version is available from the school.

Filtering and Monitoring Compliance Statement (KCSIE 2026)

System Architecture: Smoothwall S5 (On-Premise Appliance) with Smoothwall Cloud Filter

Review Cycle: Annually (Every September)

Applicable Guidance: DfE Keeping Children Safe in Education (KCSIE 2026) & UK SIC Appropriate Filtering Standards

1. System Scope & Architecture

Our school utilizes a hybrid safeguarding approach by anchoring network infrastructure to a **Smoothwall S5 On-Premise Appliance** paired dynamically with **Smoothwall Cloud Filter**. This configuration ensures seamless protection:

- **On-Premise & Off-Site Security:** The S5 appliance secures all standard on-site hardware and backup failovers. The Cloud Filter extension actively protects school-managed mobile devices (e.g., laptops, tablets) when operating remotely or connecting via portable Wi-Fi / home networks.
- **Identity-Based Logic:** User authentication passes directory details into the Smoothwall Cloud service. This applies targeted, age-appropriate filtering policies mapped directly to the individual student or staff profile.

2. Meeting the Four Areas of Risk

The architecture effectively blocks, intercepts, and flags digital activity across the four statutory risk categories outlined by KCSIE:

- **Content:** Real-time web filtering and safe-search enforcement block exposure to illegal, harmful, or inappropriate materials.
- **Contact:** The system restricts unauthorized communication channels, peer-to-peer applications, and unapproved chat networks.
- **Conduct:** Content modification and cloud scanning tools flag cyberbullying, hate speech, and the creation or sharing of harmful user-generated materials.
- **Commerce:** Active blocks protect against commercial exploitation, gambling, and financial scams.

3. Advanced 2026 Technical Compliance

In accordance with the latest DfE mandates, our system meets advanced session-analysis standards:

- **Generative AI & Deepfakes:** Smoothwall's engine actively evaluates session-generated code. It identifies and filters dynamic, personalized content—such as generative AI chat outputs and synthetic deepfakes—that standard URL blocklists fail to catch.
- **Decryption & SSL Inspection:** The S5 appliance performs granular HTTPS inspection to read web traffic text safely, ensuring encrypted sessions do not hide safeguarding risks.
- **Cloud Infrastructure Scans:** The system utilizes [Smoothwall Cloud Scan](#) to run daily sweeps across school-managed cloud storage areas, identifying hidden or AI-generated nudes/semi-nudes and alerting the DSL team instantly.

4. Oversight, Governance, and Review Schedule

Safeguarding remains a leadership responsibility supported by technology, rather than an outsourced IT function:

- **Annual September Review:** The Governing Body, Senior Leadership Team (SLT), and Designated Safeguarding Lead (DSL) conduct an extensive [Filtering System Review](#) every **September**. This maps system performance against the updated academic year's KCSIE guidelines.
- **Interim Testing:** Technical staff conduct routine checks between annual reviews using diagnostic tools (such as [testfiltering.com](#)) across a representative variety of school devices to ensure policies stay active and functional.
- **Reporting Accessibility:** The DSL team utilizes line-by-line metrics from [Smoothwall Cloud Reporting](#) to review daily activity alerts, optimize over-blocking, and evaluate systemic trends.