Red Hall Primary School

Filtering and Monitoring Policy

IT Policy Document

Version 1.0

School:	Red Hall Primary School
Approved by:	Governing Body
Date approved:	September 2026
Next review date:	September 2028

1. Introduction

Effective filtering and monitoring of internet content is a critical component of the school's approach to safeguarding and online safety. The filtering of internet content helps to prevent users from accessing material that is illegal or inappropriate in an educational context, while monitoring enables the school to identify and respond to potential safeguarding concerns.

This policy is informed by the DfE's Keeping Children Safe in Education 2026 (KCSIE), the DfE's Digital and Technology Standards (Filtering and Monitoring Standards), and the UK Safer Internet Centre's Appropriate Filtering and Monitoring Definitions (2025).

No filtering or monitoring system can provide a 100% guarantee against accessing inappropriate content. Filtering and monitoring must therefore be understood as one element within a broader strategy for online safety, which includes education, supervision, and clear policies.

2. Purpose

This policy aims to:

- Ensure the school meets the DfE's Filtering and Monitoring Standards for Schools and Colleges.
- Establish clear roles and responsibilities for the management of filtering and monitoring systems.
- Protect all users from accessing illegal, harmful, and inappropriate content.
- Enable the identification and escalation of safeguarding concerns through effective monitoring.
- Ensure filtering and monitoring systems are regularly reviewed and updated.
- Address emerging risks including those posed by generative AI tools.

3. Scope

This policy applies to all users of the school's network and devices, including staff, pupils, governors, volunteers, visitors, and any guest users. It covers:

- All school-owned devices.
- All devices using the school's broadband connection.
- Personal devices (BYOD) when connected to the school network.
- All internet feeds, including any backup connections.
- Mobile and app-based content accessed through school systems.

4. Legal and Regulatory Framework

- DfE (2026) 'Keeping Children Safe in Education 2026'
- DfE (2025) 'Meeting Digital and Technology Standards in Schools and Colleges' – Filtering and Monitoring Standards
- UK Safer Internet Centre 'Appropriate Filtering and Monitoring Definitions' (2025)

- DfE (2025) ‘Generative AI: Product Safety Expectations’
- Counter-Terrorism and Security Act 2015 (Prevent Duty)
- Data Protection Act 2018 and UK GDPR
- Online Safety Act 2023

5. Roles and Responsibilities

The DfE's Filtering and Monitoring Standards require schools to identify and assign clear roles and responsibilities:

Role	Responsibilities	Assigned To
Responsible Governor	Strategic oversight of filtering and monitoring; receiving assurance that standards are being met.	David Bell
Senior Leader	Ensuring standards are met; procuring systems; documenting decisions on what is blocked/allowed and why; reviewing effectiveness.	Helen Tomlinson
Designated Safeguarding Lead (DSL)	Understanding filtering and monitoring systems; receiving and acting on monitoring alerts; ensuring monitoring supports safeguarding.	Helen Tomlinson
IT Provider	Day-to-day management of filtering and monitoring systems; providing reports; maintaining and updating systems; testing effectiveness.	Network IT 24

6. Filtering

6.1 Filtering Standards

The school's filtering system must meet the following requirements, as set out in the DfE's standards and the UK Safer Internet Centre's 2025 definitions:

- Filter all internet feeds, including any backup connections.
- Be operational, up to date, and applied to all users, including guest accounts.
- Be applied to all school-owned devices and all devices using the school broadband connection.
- Block illegal content (including CSAM) without the option to disable.
- Be age-appropriate and suitable for educational settings.
- Handle multilingual web content, images, common misspellings, and abbreviations.
- Identify and block technologies that allow users to circumvent filtering, such as VPNs, proxy services, and end-to-end encryption methods.
- Identify and block portable Wi-Fi devices (personal hotspots) that could be used to bypass school filtering.
- Provide alerts when web content has been blocked.
- Effectively and reliably prevent access to harmful and inappropriate content generated by generative AI systems, in line with the UK Safer Internet Centre's 2025 definitions.
- Address misinformation and disinformation, which are now within the scope of filtering (2025 update).

6.2 Mandatory Blocklists

The following blocklists must be in place and cannot be disabled or overridden:

- **Internet Watch Foundation (IWF) URL list:** blocks known child sexual abuse material (CSAM). This list cannot be disabled.
- **Counter-Terrorism Internet Referral Unit (CTIRU) list:** blocks terrorist and extremist content. This list cannot be disabled.

The IT provider must confirm that both blocklists are active and cannot be disabled by any user.

6.3 Filtering Categories

In addition to the mandatory blocklists, the filtering system will block access to content in the following categories:

- Child sexual abuse material (CSAM) – always blocked via IWF list, cannot be overridden.
- Terrorist and extremist content – always blocked via CTIRU list, cannot be overridden.
- Content promoting self-harm and suicide.
- Pornographic and sexually explicit material.
- Violence and hate speech.
- Illegal content.
- VPNs, proxy services, and circumvention tools.
- AI tools and generative AI platforms not approved for school use.
- Age-inappropriate content.

6.3 Managing Filtering Requests

Where staff need access to content that is blocked by the filter for legitimate educational purposes:

- A request must be made to the senior leader responsible for filtering.
- The request must be documented, including the reason, the content, and the intended audience.
- The senior leader will approve or deny the request, with reasons recorded.
- Where approved, access should be time-limited and monitored.
- A record of all overrides and exceptions must be maintained for review.

7. Monitoring

7.1 Monitoring Standards

The school's monitoring strategy is informed by the filtering and monitoring review and includes:

- Physical monitoring: staff observing pupils' screens during lessons and activities.
- Device management software: allowing staff to view and control pupil devices during lessons.
- Network monitoring: logging internet traffic and web access.

- Individual device monitoring: through software or third-party services that generate alerts for safeguarding concerns.
- AI interaction logging: monitoring systems maintain robust activity logging for interactions with generative AI tools, in line with the UK Safer Internet Centre's 2025 definitions.

7.2 Monitoring Reports and Alerts

The monitoring system will generate reports and alerts as follows:

- **Weekly monitoring reports:** The IT provider will produce weekly monitoring reports highlighting all incidents. These will be reviewed by the DSL and the senior leader responsible.
- **Real-time high-risk alerts:** Safeguarding alerts (e.g. searches related to self-harm, exploitation, extremism) and malicious/technical incidents will be escalated to the DSL immediately.
- Policy violation alerts (e.g. attempts to access blocked content, circumvention attempts) will be reported to the senior leader responsible.
- The DSL will assess all safeguarding alerts and determine the appropriate response, following the school's safeguarding procedures.
- All alerts and responses will be recorded, including any false positives.

7.3 Staff Monitoring

Staff should be aware that their activity on school systems is monitored and logged. This monitoring is conducted in line with the school's Acceptable Use Agreement and data protection requirements. Staff will be informed of the monitoring arrangements at induction.

8. Password Security

A secure authentication system underpins effective filtering and monitoring. The school's password policy reflects NCSC and DfE guidance:

- All passwords must be at least 12 characters long; users are encouraged to use three random words.
- Complexity requirements are not used, in line with NCSC guidance.
- Passwords do not expire routinely but are changed immediately if compromised.
- Multi-factor authentication (MFA) is required on all accounts with access to sensitive or personal data.
- Common passwords are blocked and brute-force protections are in place.
- No default passwords remain on any system.
- All users are responsible for the security of their credentials and must report any suspected breach immediately.

Detailed password guidance for learners and further provisions are set out in the Cyber Security Policy.

9. Vulnerable Groups

The school recognises that some pupils may be more vulnerable to online risks. The filtering and monitoring provision will take account of:

- Pupils with SEND, who may face additional online risks including from bullying, grooming, and radicalisation.
- Pupils with English as an Additional Language (EAL).
- Younger pupils who may need additional protections.
- Pupils identified as at particular risk through the school's safeguarding processes.

Where individual filtering exceptions are needed for specific pupils, these must be documented with a clear justification and approved by the DSL.

10. Mobile and App Content

Mobile and app content is often presented differently to web browser content. The school will:

- Confirm with the IT provider whether the filtering system covers mobile and app-based content.
- Apply monitoring to devices accessing mobile or app content to reduce the risk of harm.
- Restrict or block app installations on school devices where appropriate.

11. Technical Security

In addition to filtering and monitoring, the school's technical security measures include:

- All technical systems are managed to meet DfE recommended standards.
- Cyber security is included on the school's risk register.
- Servers, wireless systems, and cabling are physically secured with restricted access.
- Air-gapped or off-site backups are maintained.
- Anti-malware software is up to date across all devices.
- Users do not have administrator access to school devices by default.
- Guest users are provided with appropriate, risk-assessed access.
- Software licences are accurate and regularly audited.
- Personal data cannot be sent over the internet or taken off-site unless securely encrypted.

Full details are set out in the Cyber Security Policy.

12. Annual Review of Filtering and Monitoring

The DfE requires that filtering and monitoring provision is reviewed at least annually. The review will be conducted by:

- The senior leader responsible for filtering and monitoring.
- The DSL.
- The IT provider.
- The responsible governor.

The review will consider:

- Whether the filtering system meets the DfE's standards and the UK Safer Internet Centre's definitions.
- Whether the monitoring system is effectively identifying and escalating safeguarding concerns.
- Filtering and monitoring logs and incident reports.
- New and emerging risks, including those from generative AI and new technologies.
- User feedback and survey results.
- Whether any changes to systems, providers, or configurations are needed.
- The needs of vulnerable pupil groups.
- BYOD policies and coverage.

The outcome of the review will be recorded and reported to the governing body.

13. Monitoring and Review of This Policy

This policy will be reviewed at least annually, or more frequently in response to:

- Changes in the DfE's Filtering and Monitoring Standards or KCSIE.
- Updates to the UK Safer Internet Centre's definitions.
- Significant new technological developments or threats.
- Serious online safety incidents.

Changes will be communicated to all members of the school community.

14. Further Information

- DfE Filtering and Monitoring Standards: gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- UK Safer Internet Centre Filtering and Monitoring Guidance: saferinternet.org.uk
- NCSC Cyber Security Guidance for Schools: ncsc.gov.uk/section/education-skills/schools
- DfE KCSIE 2026: gov.uk/government/publications/keeping-children-safe-in-education