

# Filtering & Monitoring Policy

September 2024



**Limitless Potential**

**Ignite Passion**

**Embrace Difference**

Mr. Stephane Bommel  
Headteacher

Mr. Keith Oliver  
Chair of Governors

## Filtering & Monitoring Policy

---

**Hazlewood Community Primary School**

*Date: September 2024*

*Date for Governors Review: September 2025*

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'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. Whilst internet filtering has always been provided by schools, it is the 'strengthened measures' that are now a key part of Ofsted online safety during inspections. 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. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

### **Aims and Objectives**

This policy aims to identify and assign roles and responsibilities to manage and review filtering and monitoring systems and to put effective monitoring strategies in place that meet Hazlewood Community Primary School safeguarding needs.

Legislation and statutory guidance This policy is based on the Department for Education's statutory guidance Keeping Children Safe in Education (2023) and Statutory guidance on the Prevent duty, which explains schools' duties under the Counter-Terrorism and Security Act 2015 with respect to protecting people from the risk of radicalisation and extremism This policy applies to all staff, governors and visitors to the school.

Requirements of Online Filtering and Monitoring Hazlewood Community Primary School follows the Department for Education Filtering and Monitoring Standards for Schools and Colleges.

[Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK](#)

## **Roles and Responsibilities**

### **All staff will:**

- Ensure that they follow school policy regarding appropriate use of the internet and that they use the school reporting mechanisms to alert senior leaders and the IT technician of any breaches in filtering and monitoring systems.
- Be aware of Hazlewood Community Primary School's systems supporting safeguarding, including this Filtering and Monitoring policy, the staff Code of Conduct, the Positive Behaviour for Learning Policy, IT acceptable use policy, The Prevent Duty and Safeguarding and Child Protection Policy.
- Understand the process for making referrals to the Prevent Duty, including the role they might be expected to play.
- Be able to identify the signs of child-on-child abuse, child sexual exploitation (CSE), child criminal exploitation (CCE), indicators of being at risk from or involved with serious violent crime, radicalisation and serious violence (including that linked to county lines).
- Inform the DSL and IT provider if they will be covering content in classes that could create unusual activity on filtering logs (eg: World War II, Nazi Germany)

### **All staff should report to DSL and IT provider if:**

- They witness or suspect unsuitable material has been accessed
- They can access unsuitable material
- There is a failure in the software or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- They notice abbreviations or misspellings that allow access to restricted material

### **The Senior Leadership Team are responsible for:**

- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of provision alongside the DSL and IT provider
- Overseeing reports
- Ensuring that staff understand their role, are appropriately trained, follow policies, processes and procedures, acts on reports and concerns.

Senior leaders should work closely with governors or proprietors, the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective.

### **The Designated Safeguarding Lead:**

The Designated Safeguarding Lead will take responsibility for safeguarding and online safety, including overseeing:

- Producing filtering and monitoring reports
- Safeguarding concerns
- Carrying out checks and reviews to filtering and monitoring systems alongside SLT and IT providers, with support from allocated governors.
- Ensuring that suitable staff training is provided

### **The IT service provider:**

The IT service provider has technical responsibility for maintaining filtering and monitoring systems, providing filtering and monitoring reports and completing actions following concerns or checks to systems.

### **The IT service provider should work with the senior leadership team and DSL to:**

- Procure systems
- Identify risks
- Carry out reviews
- Carry out checks
- Check that filtering and monitoring systems work on new devices and services before releasing

### **The Headteacher will:**

The Headteacher will ensure that the policies and procedures adopted by the Governing Body are effectively implemented and followed by all staff (including temporary staff and volunteers) as part of their induction and that they understand and follow the procedures outlined in this policy. This policy is communicated to parents/carers when their child joins the school and via the school website

- Make decisions regarding all low-level concerns, collaborating with the DSL on this.
- All staff and volunteers feel able to raise concerns about poor or unsafe practice in regard to children, and such concerns are addressed sensitively and effectively in a timely manner. The NSPCC whistle blowing helpline number is also available (0800 028 0285). Also see Hazlewood Community Primary School Whistle Blowing Policy.
- If there is a concern or complaint about the Headteacher, the Chair of Governors must be contacted. The contact details for the Chair of Governors is located at the school reception. If there is a concern about the Head Teacher, the Chair of Governors must be contacted in writing.

Please address your letter c/o Clerk to the Governors at the school address or email

[office@hazlewoodprimary.co.uk](mailto:office@hazlewoodprimary.co.uk)

## **Governing Body:**

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

## **Reviewing Filtering and Monitoring Systems**

SLT, the DSL, IT provider and responsible governor will carry out and record annual checks of the filtering and monitoring systems as follows:

- Check filtering systems, including school owned devices and services and those used off site
- Evaluate changing and updated risks
- Review risk profile of students, localised risk and external safeguarding influences (eg: county lines)
- Review current filtering systems, considering what has been blocked and why
- Consider relevant safeguarding reports over the last year
- Review the digital resilience of students as a group
- Consider school's approach to young people accessing 3G, 4G and 5G in school
- Review Prevent Duty risk assessment

## **Records and Monitoring**

Well-kept records are essential to good child protection practice. All staff are clear about the need to record and report concerns about a child or children within the school and have training using CPOMS.

Records of concerns are written down or typed, signed and dated and passed immediately to the Designated Safeguarding Lead (or a Deputy). The Designated Safeguarding Lead is responsible for such records and for deciding at what point these records should be passed over to other agencies (in accordance with the Data Protection Act 2018 and GDPR Principles)

- Breaches of filtering and monitoring systems should be reported on the school's 'Child Protection Online Monitoring System' CPOMS and should be reported directly to the IT technician.
- Child protection records are stored securely on our CPOMS online system, with access confined to specific staff, eg the Designated Safeguarding Lead (and relevant deputies) and the Headteacher.

## **Extremism**

If a child is not suffering or likely to suffer from harm, or in immediate danger, where possible speak to the DSL first to agree a course of action.

If in exceptional circumstances the DSL is not available, this should not delay appropriate action being taken.

Speak to a member of the senior leadership team and/or seek advice from local authority children's social care. Make a referral to local authority children's social care directly, if appropriate (see 'Referral' above).

Inform the DSL or deputy as soon as practically possible after the referral.

Where there is a concern, the DSL will consider the level of risk and decide which agency to make a referral to. This could include Channel, the government's programme for identifying and supporting individuals at risk of being drawn into terrorism, or the local authority children's social care team.

The Department for Education also has a dedicated telephone helpline, 020 7340 7264, which school staff and governors can call to raise concerns about extremism with respect to a pupil. You can also email [counter.extremism@education.gov.uk](mailto:counter.extremism@education.gov.uk).

Note that this is not for use in emergency situations.

In an emergency, call 999 or the confidential anti-terrorist hotline on 0800 789 321 if you:

- Think someone is in immediate danger
- Think someone may be planning to travel to join an extremist group
- See or hear something that may be terrorist-related