

Hempshill Hall Primary School



Filtering and Monitoring Policy

September 2026

This Filtering & Monitoring policy has been written with consideration to KCSIE 2026).

1. Introduction

This filtering and monitoring policy outlines the guidelines and procedures for monitoring and filtering information accessed by students, staff, and visitors within Hempshill Hall Primary school. The policy aims to ensure a safe and secure learning environment while promoting responsible and appropriate use of digital resources.

2. Purpose

The purpose of this policy, which should be read alongside our Online Safety Policy is to:

- a. Safeguard students from accessing harmful or inappropriate content.
- b. Protect the school's network and computer systems from security threats.
- c. Encourage responsible and ethical use of digital resources.
- d. Comply with relevant legal and regulatory requirements.

3. Responsibilities

- a. School Administration: The school administration is responsible for implementing and enforcing this policy, including selecting and maintaining appropriate filtering and monitoring tools, and providing necessary training to staff.
- b. Staff: Staff members must promote responsible and safe use of digital resources, monitor students' online activities during school hours, and report any concerns or incidents to the appropriate authorities.
- c. Students: Students must use digital resources responsibly and follow the school's guidelines for acceptable online behaviour. They should report any inappropriate content they come across to their teacher or a trusted adult.

4. Decision Making

- a. Hempshill Hall Primary School governors have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks.
- b. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- c. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- d. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- e. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- f. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

5. Filtering and Monitoring Tools

- a. The school will implement appropriate filtering and monitoring tools to restrict access to websites and content that are deemed inappropriate, harmful, or unrelated to educational purposes. For this purpose, we use staff vigilance, Netsweeper (filtering) and Smoothwall (monitoring).
- b. The filtering system will be regularly updated and configured to block or filter categories such as violence and gore, sexual content, offensive behaviour, racism and hate speech, and other potentially harmful materials.
- c. The school will also implement monitoring tools to monitor students' online activities, which may include tracking websites visited, search queries, and email communications. This monitoring will be conducted in compliance with applicable privacy laws and regulations.

Filtering

- We use Netsweeper which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- If learners discover unsuitable sites, they will be required to:
 - Turn off monitor/screen and report the concern immediate to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Nottingham Police or CEOP.

Monitoring

- We use Smoothwall Monitoring software to provide appropriate monitoring of pupils and staff. Email alerts are sent to DSL staff when a threshold is breached (depending on Event Type) for concerning online behaviour.
- We appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
 - Physical monitoring (supervision), Smoothwall monitoring of internet and web access.
- If a concern is identified via monitoring approaches, the DSL or deputy will:
 - Respond in line with the child protection policy.

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6. Acceptable Use and Online Behaviour

- a. The school provides clear guidelines to students and staff regarding acceptable use of digital resources, including rules on accessing and sharing appropriate content, cyberbullying, online privacy, and copyright infringement.
- b. Students and staff are expected to use digital resources in a responsible, respectful, and ethical manner.

c. Online communication, including email and social media use, should be conducted professionally and responsibly, with appropriate language and tone.

See the school's Acceptable Use Policy for further detail and guidance.

7. Reporting and Response Procedures

- a. Staff members should promptly report any concerns or incidents related to inappropriate or harmful content to the designated authority within the school (Jon Wright and Schools IT).
- b. Reported incidents will be thoroughly investigated, and appropriate actions will be taken to address the situation, which may include parental involvement, disciplinary actions, or involvement of external authorities if necessary.
- c. Students, staff, and parents should be encouraged to report any potential breaches of this policy or incidents they come across.

8. Training and Education

- a. The school will provide regular training and education sessions for staff, students, and parents to raise awareness about safe and responsible use of digital resources, including the potential risks and consequences associated with inappropriate behaviour online.
- b. Training will also cover identifying and reporting online safety concerns, understanding the importance of privacy and data protection, and promoting positive digital citizenship.

9. Review and Amendments

- a. This policy will be reviewed periodically to ensure its effectiveness and compliance with legal and regulatory requirements.
- b. Amendments to the policy may be made as necessary, with proper communication and training provided to staff, students, and parents.
- c. Feedback and suggestions from stakeholders will be considered during the policy review process.

10. Policy Dissemination

- a. This policy will be communicated to all staff, students, and parents, and a copy will be made available on the school's website.
- b. Any updates or changes to the policy will be promptly communicated to relevant stakeholders.
- c. Acknowledgment of receipt and understanding of this policy may be required from staff, students, and parents.

10. Compliance

- a. Failure to comply with this policy may result in disciplinary action, which may include restricted access to digital resources, loss of privileges, or other appropriate measures.
- b. Breaches of this policy may also result in the involvement of external authorities, as required by law.

11. Conclusion

This Filtering and Monitoring Policy aims to create a safe and secure online environment for students, staff, and visitors within UK primary schools. By promoting responsible and ethical use of digital resources and implementing appropriate filtering and monitoring measures, the policy ensures that students can access educational content while protecting them from potentially harmful or inappropriate material.

To be reviewed in September 2027