Snowflake School

'Improving the quality of family life'

Filtering and Monitoring Policy

Contents

Purpose

This policy outlines our approach to internet filtering and monitoring at Snowflake School. Given our 1:1 supervision, the policy focuses on ensuring a safe online environment while addressing the specific needs of our pupils. It outlines the steps our school will take to manage and respond to breaches detected by the online filtering system.

Our pupils may have limited awareness of online risks and require enhanced supervision, support, and personalised teaching to develop digital resilience appropriate to their stage of understanding. This is particularly important for pupils with autism and other SEND, who may be more vulnerable to grooming, manipulation, or fixation on specific online interests.

The aim is to safeguard pupils, staff and visitors accessing the school's network and internet services, while complying with statutory guidance, including Keeping Children Safe in Education (KCSIE) and the DfE's Filtering and Monitoring Standards.

Roles and Responsibilities

- **Designated Safeguarding Lead (DSL)**: Oversight of online safety, oversees the monitoring and response process, breach escalation and liaises with external agencies when required.
- **Senior Leadership Group (SLG)**: Ensures compliance with this policy and provides the necessary resources for implementation, monitors daily reports, ensures staff training.
- **IT support team**: Maintains Smoothwall system, implements technical measures to enhance filtering, maintains logs of all safety breaches
- **All staff:** Must report any filtering alerts or inappropriate use of technology to the DSL / DDSL immediately.

The DSL will produce an annual filtering and monitoring report to governors/trustees detailing incidents, trends, system performance, and staff training outcomes.

- **Trustees:** Review policy implementation annually. A nominated trustee with the responsibility for safeguarding will oversee compliance and receive an annual report from the DSL/SLG.

Measures in place for Online Safety

- **Supervision**: Pupils are supervised 1:1 during all digital activities to minimize exposure to risks and to ensure appropriate use of technology. Devices (iPad, tablets, laptops and computers) are only used when supervised by an adult.
- **Educational Content**: Online tools and resources are pre-vetted for suitability, and staff remain vigilant during their use.

Online safety is embedded in the curriculum at an appropriate cognitive level for pupils, using social stories, visuals, and repetition to reinforce safe online behaviours. Parents and carers are provided with information and training on online safety at least annually, including guidance on managing devices at home and supporting safe online habits.

- **Pupil Education**: Age-appropriate lessons on safe and responsible internet use are incorporated into the curriculum including during PSHE and part of Internet Safety Day.

Filtering and Monitoring system

Filtering systems block access to harmful websites and content. Monitoring systems identify when someone searches for or accesses certain types of harmful online content on school devices, identify who is searching for or accessing the harmful content and alerts the school about it so we can intervene and respond. The school uses **Smoothwall Safeguarding** as its internet filtering and monitoring solution.

Smoothwall incorporates an alerting service that notifies safeguarding leads of any filtering and safeguarding breaches. This alerting system proactively informs stakeholders, even if the content has not been configured to be blocked, allowing for prompt review of policies and response to potential risks. Each filtering log is time stamped with the precise date and time of the attempted access. Smoothwall diligently records all search terms and blocked websites, making this information readily accessible through its alerting and reporting platforms.

Levels of Filtering

1- Maximum filter. This is for all pupils' devices

2- Medium Filtering – For middle leaders. Access to platforms like YouTube/Zoom and similar sites is allowed, so they are able to plan work. Requests for additional access must be submitted by email and approved by SLG before IT adjusts the filter.

3- Minimum filtering for senior leaders. Senior leaders can access majority of sites. If any report shows that there was access to unwanted sites our IT support can check and block the site.

Smoothwall provides:

- **Daily Reports**: Smoothwall generates daily reports highlighting breaches or attempts to access dangerous content.
- **Categories of blocked content such as**:
    - Illegal content (e.g., child abuse material, extremism, hacking, weapons, drugs)
    - Inappropriate content (e.g., adult material, violence, hate speech, ..)
    - Content unsuitable for educational purposes (e.g., gaming, social media, and dating).

Smoothwall has a long-standing partnership with the Internet Watch Foundation (IWF), enabling Smoothwall to create digital safety solutions that are designed to keep harmful images away from young or vulnerable adults. The CAIC list of domains and URLs is an integral part of Smoothwall Filter. A number of search terms and phrases provided by the IWF, and perform daily self-certification tests to ensure the IWF content is always blocked through a Smoothwall Filter.

Response to Filtering Breaches

Daily reports are reviewed by DSL/DDSL to identify patterns or concerns. The following steps are taken when filtering breaches are identified and flagged as dangerous or concerning.

1. Automated alerts from the filtering system are logged in Smoothwall
2. Staff detecting a breach in person must report it to the DSL / DDSL immediately and log it on MyConcern, including:
    - URL or content in question
    - User
    - Device used
    - Date and time of the incident
3. DSL / DDSLs reviews the breach to make an initial assessment and classify it as:
    - Low risk: Accidental access or minor inappropriate content.
    - Moderate risk: Deliberate but non-threatening inappropriate use.
    - High risk: Serious content (e.g., illegal material, cyberbullying, threats).
4. Actions
    - Block URL/content immediately.
    - Suspend user's access if necessary.
    - Record the evidence.
    - For moderate or high-risk breaches:
        - Notify parents/carers by phone call followed up in writing for pupil related incidents.
        - For illegal content or significant safeguarding concerns, report to relevant external agencies or authorities. (CEOP, police, Local Authority)
    - Investigate the incident as appropriate.
    - Update filtering and monitoring settings as required to prevent recurrence.
    - Record outcomes in safeguarding records (MyConcern)

Where a member of staff is involved in a breach, this will be managed in accordance with the Staff Code of Conduct and Disciplinary Policy, alongside safeguarding procedures if appropriate.

All data captured by the filtering and monitoring system is stored securely, accessed only by authorised staff, and retained in accordance with GDPR and the school's Data Protection Policy.

- Hold an all staff meeting and remind them of online safety and Safeguarding

Staff Training and awareness

All staff receive annual training on this policy, online safety protocols and safeguarding in a digital context, which includes:

- Each member of staff has to sign an acceptable IT use agreement
- Understanding the scope of Smoothwall filtering- staff information sheet.
- Recognizing and responding to online safety risks.
- Using monitoring reports effectively.
- Managing and supporting pupils' online activities responsibly.

Staff are provided with resources and support to address new online threats or technologies. Regular updates on emerging risks and changes to filtering protocols are shared during staff meetings or via email. We ensure that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks. Staff are also aware of the need to prevent 'over blocking' of content as that may unreasonably restrict what can be taught with regards to online activities and safeguarding.

Users must not attempt to use any programmes or software that will allow them to bypass the filtering systems in place to prevent access to such materials. To prevent users from bypassing the filtering system, Smoothwall filter contains specific categories to block VPN technologies and proxy services. These categories are applied using both /domain filtering and page construction analysis, enabling detection of unknown or new sites and technologies that attempt to circumvent filtering measures.

In the event of a system outage or internet failure, staff must suspend online activities until the filtering and monitoring system is confirmed as operational.

All staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils. Effective classroom management and regular education about safe and responsible use is essential.

Policy review

The school will commission an annual technical audit of filtering and monitoring effectiveness, either through the IT provider or an independent assessor, to ensure systems remain robust and compliant with DfE standards.

The review should be conducted by members of the SLG, the DSLs, and the IT service provider, and the nominated safeguarding trustee. The review will ensure continued compliance with statutory guidance and responsiveness to new risks and technologies.

Revision

Version Update	October 2025
Review due	October 2026
Reviewed By	Sumen Starr
Approved by Board of Trustees on	October 2025