OUR APPROACH TO FILTERING AND MONITORING

Updated: February 2026

1. Introduction

St Peter and St Paul CE Primary School is committed to keeping all **children**, staff, volunteers, and visitors safe when using digital technologies. Effective **filtering and monitoring** is a statutory safeguarding requirement, forming part of our wider online safety and child protection responsibilities. This approach aligns with:

- **Keeping Children Safe in Education (KCSIE) 2025**, which requires all staff to receive online safety training, including clear expectations relating to filtering and monitoring systems.
- The school's **Online Safety Policy**, which outlines how filtering, monitoring, and acceptable use form part of our safeguarding culture.

---

2. Purpose of Filtering and Monitoring

Our filtering and monitoring systems exist to:

- Protect children from **content, contact, conduct, and commercial** online risks.
- Ensure safe and appropriate use of digital tools, including AI.
- Enable the school to identify and respond to online safety concerns swiftly.
- Support statutory safeguarding responsibilities by helping staff recognise patterns of behaviour that may indicate risk or abuse.

---

3. Filtering Systems

The school uses **Cisco Meraki** and **SENSO** to provide robust, role-based protection.

3.1 How Filtering Works

The filtering system:

- Categorises websites and online content by risk type.
- Automatically blocks access to harmful or illegal content, including extremism, pornography, discrimination, self-harm, unsafe AI, gambling, malware, scams, and other inappropriate material.
- Applies different rules depending on user role (child, staff, visitor) and device type.

3.2 Age and Role-Based Controls

Enhanced restrictions apply for children, including blocking or limiting:

- Social media (unless required for curriculum use)
- Anonymous communication tools
- Unsafe or unregulated AI platforms
- High-risk categories of content

---

4. Monitoring Systems

4.1 How Monitoring Works

Our monitoring system (SENSO):

- Records internet activity and keystrokes on school-managed devices.
- Flags concerning search terms, unsafe behaviour, attempts to bypass filters, cyberbullying indicators, and safeguarding-related risks.
- Links logs to the authenticated user and device, enabling accurate follow-up.

KCSIE emphasises the ongoing safeguarding importance of monitoring children's online behaviour, including risk of child-on-child abuse, exploitation, and online grooming.

4.2 Access to Monitoring Data

Monitoring information is accessed only by:

- Headteacher
- Designated Safeguarding Lead (DSL) and Deputies
- IT provider (Education Lincs Ltd), for technical purposes

All data is stored securely and used proportionately.

---

5. Responsibilities

5.1 Governing Body

Governors must ensure:

- Filtering and monitoring systems are appropriate and effective.
- Online safety is part of whole-school safeguarding practice.

5.2 Headteacher

The headteacher ensures staff understand and apply filtering and monitoring expectations as part of mandatory safeguarding training.

5.3 Designated Safeguarding Lead (DSL)

The DSL:

- Reviews alerts and incidents.
- Coordinates responses, including risk assessments, parent communication, pastoral support, or referrals to agencies where required.
- Oversees incidents involving misuse of digital tools or AI.

5.4 Staff

Staff must:

- Comply with Acceptable Use Agreements.
- Supervise children during technology use.
- Model responsible digital behaviour.
- Report online safety concerns immediately.

5.5 Children

Children are taught:

- To use technology safely, respectfully and responsibly.
- That their activity may be monitored.
- To report concerns promptly to trusted adults.

---

6. AI-Related Filtering and Monitoring

The school recognises new risks associated with artificial intelligence.

We therefore ensure that:

- Unsafe or unregulated AI tools are blocked.
- AI use is monitored for safety and ethical compliance.
- Children are taught about AI limitations, risks, and responsible use.
- Misuse of AI tools is treated seriously and managed in line with safeguarding and behaviour policies.

---

7. Use of Google for Education

St Peter and St Paul CE Primary School uses **Google for Education** to support teaching, learning, and secure communication.

7.1 User-Based Policies

Google accounts are governed by age- and role-specific settings:

- Different permissions for children, staff, leaders, and administrators.
- Additional restrictions for children, including blocked apps, add-ons, and limited AI features.
- Activity logging consistent with the school's wider monitoring expectations.

7.2 Device-Based Policies (Chrome Management)

The school applies granular controls through Chrome Management, including:

- Enforced SafeSearch
- Restricted extensions
- Blocked developer tools
- Automatic system updates
- Policies applying on-site and off-site

These ensure protection and compliance wherever devices are used.

7.3 Integration with Filtering and Monitoring

Google for Education integrates seamlessly with Cisco Meraki and SENSO so that:

- Filtering continues across Google services such as Search, YouTube, Drive, and Workspace apps.
- Attempts to access dangerous content within Google tools trigger monitoring alerts.
- User behaviour remains visible to senior leaders and DSLs when safeguarding concerns arise, supporting the expectations for filtering and monitoring under KCSIE.

---

8. Responding to Incidents

When monitoring systems highlight a concern, the DSL or Headteacher will:

- Review the incident and context
- Speak with the child or staff member involved
- Inform parents where appropriate
- Complete a risk assessment
- Provide pastoral or behavioural support
- Take disciplinary action if needed
- Refer to external agencies (e.g., police) if illegal content is involved

This reflects the requirement that concerns are acted on **immediately** and in the child's best interests. It is also consistent with the Online Safety Policy's behaviour, misuse, and incident-handling procedures.

---

9. Transparency With Parents

Parents are informed about:

- The nature of filtering and monitoring systems
- How these systems help keep children safe online
- How incidents are responded to

This supports open communication and shared responsibility for children's safety.

---

10. Review of Filtering and Monitoring

The school reviews filtering and monitoring arrangements:

- At least annually
- After any serious safeguarding incident
- When new technology or risks emerge (e.g., developments in AI)

The Headteacher, Governors, DSL, and IT provider collaborate to ensure systems remain effective and up to date.