St Philip's CE
PRIMARY SCHOOL

## Network and Mobile Device Security

### What filters do we have?

The School has a filtering solution from Net Sweeper who along with other providers have details of how they meet the checklist standards asked for by the DFE Digital Standards Guidance.

The following links provide additional information

- https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- https://assets.publishing.service.gov.uk/media/6a9081309a177a1decf97b00/Keeping_children_safe_in_education_2026.pdf
- https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-responses-0

We use a cloud-based system, devices used at home provided by the school to adults and children will still be filtered by the schools' solution. Each user has an individual home log in for ease of identity.

The Net Sweeper's cloud's patented security reinforces Google Safe Search, YouTube and social media sites with advanced controls which allow us to extend safe access to these technologies without compromising the safety of our staff and pupils.

### Security:

**Mobile data devices:** All staff use Encrypted pen drives. These are registered to individuals.

**Password Mechanisms**: We use strict levels of password security and users are requested to change their passwords at regular intervals. Passwords are requested to have a set number of characters.

Two factor Authentication is in place for all staff members who log into a new device.

### Different Access Levels

The curriculum network is split in to two levels of access. The teacher has access to the following:

- Shared Drive (pupils and staff)
- Staff Drive (Staff only)
- Pupils (pupils and staff only to access pupil work)

Our Network is filtered appropriately for Primary Age Children. Where staff would like to seek access to a site that may be blocked by our usual filters the site is assessed off site by the Head Teacher and a request for the site block to be removed for the period of lesson time required for the specific class of children.

**Admin Network**

- SIMS drive (admin staff and teachers have access)
- Office shared (admin staff only)
- Personal user areas (individual user)

**Monitoring**

The school takes its monitoring responsibility seriously. To ensure we meet our responsibilities outlined in KCSIE we carry out

- All staff and children can be identified individually on our system reports making follow up straightforward.
- Daily checks of our filtering reports
- Monthly in house checks of our filtering system
- Work closely with our families to support understanding of online safety.
- Provide curriculum focused learning to ensure that children know how to report anything that they see online that concerns them.
- Children are not permitted to bring mobile phones into the classroom. All phones are handed in and stored in the school office, they are returned to children at the end of the school day or at the end of after school provision.

Filtering and monitoring systems are in real time. Requested access to blocked sites is flagged to the school office and to the Head Teacher's in the school holidays. This is a 7 day per week, 24 hr alert. A member of the office team under the supervision of the Senior Leadership team will follow up all requested access to blocked sites for both staff and children. The process for dealing with these alerts is as follows:

Alert generated → Reviewed by designated staff → Referred to DSL if safeguarding concern identified → Recorded in CPOMS where there are safeguarding concerns → Action taken in line with school policies relating to Acceptable Use or Child Protection as appropriate.

## Responsibilities

| Role | Responsibility |
|---|---|
| **Governing Board** | Strategic oversight and annual review |
| **DSL & Deputy DSLs** | Safeguarding response and monitoring concerns |
| **Headteacher** | Operational oversight |
| **APEX/IT Provider** | Technical filtering and monitoring |
| **Staff** | Reporting concerns and understanding systems |

## Emerging technologies

Filtering and monitoring arrangements will be reviewed to consider emerging technologies, including artificial intelligence tools, image manipulation technologies, social media platforms and evolving online risks. School will take advice on appropriate arrangements from the designated IT provider, APEX.

## Review Arrangements

Governors and senior leaders will review filtering and monitoring arrangements at least annually and following any significant safeguarding incident.

This document should be read in conjunction with the following linked policies:

- Child Protection & Safeguarding Policy
- Online Safety Policy
- Acceptable Use Policy
- Staff Code of Conduct
- Behaviour Policy
- Low-Level Concerns Procedure
- Use of AI Policy