

Claypole Church of England Primary School

Filtering Policy 2026 -27



Claypole C.E. Primary School uses 'SECURLY' filtering service. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Head teacher. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to the Head teacher before they take place.

School governors have overall strategic responsibility for safeguarding pupils online by ensuring their school's web filtering and monitoring systems comply with statutory guidelines like *Keeping Children Safe in Education (KCSIE)*. This involves designating a responsible governor to work with the Designated Safeguarding Lead (DSL) and IT staff to review systems at least annually

Governors do not need technical expertise, but they are expected to hold senior leaders accountable by actively challenging and verifying that systems are effective. To properly scrutinize these provisions, governors should ensure the following practices are in place:

Identify Responsibilities: Confirm that a named governor, DSL, Senior Leadership Team (SLT) member, and IT support lead have been assigned responsibility for maintaining compliance.

- **Review System Effectiveness:** Verify that the school conducts annual reviews of filtering and monitoring—or sooner if there are network changes or identified risks.
- **Ensure Non-Bypassable Protection:** Ensure the systems block illegal content (e.g., child sexual abuse material) in a way that cannot be disabled by users.
- **Evaluate Overblocking:** Check that the systems protect pupils without being so restrictive that they block legitimate, curriculum-driven content.
- **Contextual Analysis:** Ensure monitoring solutions are capable of analysing context and AI-generated content, rather than just relying on simple URL block lists.
- **Review Logs and Action Plans:** Ask for documented proof of alerts, how they were investigated, and any policy changes made as a result.

Key Changes to the Filtering Process

- **Age-Appropriate Profiles:** Different restriction levels applied to Early Years, Key Stage 1, and Key Stage 2.
- **Real-Time Analysis:** Dynamic content categorization replaces static, outdated website blocklists.
- **Search Safetynet:** Enforced "SafeSearch" mode across all search engines and video platforms.
- **Device Flexibility:** Filtering protocols now apply to school-owned devices taken home by pupils.

All users have a responsibility to report immediately to Head teacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through:

- signing the AUP (Acceptable Usage Policy)
- induction training
- staff meetings, briefings, inset/training days.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions /Induction packs etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to Head teacher who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at county level, the responsible person (Head teacher) should contact Securly Services.

References:

[Keeping children safe in education](#)

[Meeting-digital-and-technology-standards-in-schools-and-colleges](#)

[Filtering and monitoring: core standard](#)

[Cyber security: core standard](#)

Updated: August 2026 Review: October 2027

G E Doney Learning Support Manager