



Great Sampford
Primary School

Filtering and Monitoring

What is filtering and monitoring?

- Filtering systems block access to harmful or inappropriate online content on school networks and devices.
- Monitoring systems identify searches, access patterns or content on school devices or networks that may indicate a safeguarding risk. Monitoring does not itself prevent access but generates alerts so staff can intervene.
- No technical solution is 100% effective. Filtering and monitoring must be used alongside the school's safeguarding systems, behaviour policy and staff training.

Statutory context and principles

- This policy reflects the school's statutory duties in Keeping Children Safe in Education (KCSIE) and the DfE's digital and technology expectations, including the requirement that governing bodies take overall strategic responsibility for filtering and monitoring.
- The school will:
 - review filtering and monitoring at least once every academic year;
 - ensure the review is led by a named SLT member responsible for filtering and monitoring with the support of the Designated Safeguarding Lead (DSL) and IT provider;
 - keep records of checks and decisions, including checks on all internet-connected devices and locations;
 - balance blocking harmful content with not unreasonably restricting teaching and learning; and
 - consider the number and ages of pupils, pupils at greater risk, and proportionality of costs versus safeguarding risk when designing provision.

Roles and responsibilities

- Governing body (overall strategic responsibility)
 - Seek assurance that the school meets DfE filtering and monitoring standards.
 - Appoint a named governor (digital link) with responsibility for oversight of digital safety and filtering/monitoring.
 - Approve major procurement decisions and the annual filtering & monitoring review report.
- Headteacher (operational accountability)
 - Ensure roles and responsibilities are assigned and understood.
 - Appoint the SLT lead for filtering and monitoring.
 - Ensure the child protection policy and online safety policy include the school's approach to filtering and monitoring.
 - Ensure timely escalation and resourcing for remediation following any identified weaknesses.
- SLT lead for filtering & monitoring (Headteacher) – duties include:
 - lead the annual review and keep the review record;

- ensure checks are carried out on all internet-connected devices and relevant locations;
- work with the DSL and IT provider to interpret monitoring reports and decide safeguarding responses;
- maintain the "allowed/blocked" decision log with rationale;
- ensure staff receive training on their responsibilities; and
- provide an annual report to governors.

- Designated Safeguarding Lead (DSL)

- Take lead responsibility for online safety as part of overall safeguarding.
- Interpret monitoring alerts for safeguarding risk and oversee safeguarding responses, including referrals to external agencies where required.
- Ensure relevant records are retained and transferred appropriately if a pupil moves school (including any Channel/Prevent involvement).
- Work with staff to ensure curriculum and behaviour responses build pupil resilience online.

- IT service provider (external supplier – HfL)

- Implement and maintain filtering/monitoring systems.
- Provide technical checks and evidence that filtering is functioning on all internet-connected devices and in relevant locations.
- Support production of monitoring logs and configure alert thresholds in line with safeguarding needs.
- Participate in the annual review and immediate technical remediation where failures are identified.

- Teachers and support staff

- Should understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens.
- Use monitoring reports where appropriate to support pedagogical or pastoral intervention.
- Need to report safeguarding and technical concerns, such as if:
 - They witness or suspect unsuitable material has been accessed
 - They are able to access unsuitable material
 - They are teaching topics that could create unusual activity on the filtering logs
 - There is failure in the software or abuse of the system
 - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
 - They notice abbreviations or misspellings that allow access to restricted material

- The IT service provider (HfL) should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Operational practice and expectations

- Procurement and configuration

- All procurement of filtering and monitoring systems must involve the DSL, SLT lead and the named governor. Decisions must be recorded with rationale for chosen product/configuration.
 - Configurations should be risk-based, reflecting the ages and needs of our pupils, those at greater risk and the nature of curriculum use. The school will aim to block harmful content while avoiding unreasonable disruption to teaching and learning.
- Monitoring operation and response flow
 - Monitoring alerts that suggest safeguarding concerns are triaged by the DSL and SLT lead together with the IT provider.
 - Safeguarding concerns are escalated under normal safeguarding procedures; technical incidents are escalated to the IT provider for immediate remedial action.
 - The DSL is responsible for any external referrals (social care, Prevent/Channel) and for recording outcomes.
 - All actions taken in response to monitoring alerts are recorded in the school's safeguarding record (kept in line with the retention schedule).
- Checks and testing (frequency)
 - Daily: automated system health checks and alert monitoring by IT provider as configured.
 - Monthly: sampling of monitoring logs and single-device functionality checks by the IT provider.
 - Annually (minimum): full review of filtering and monitoring provision, including tests on all device types and locations (classroom devices, interactive boards, mobile devices, admin workstations, remote access, guest Wi-Fi).
- Coverage (what we check)
 - All internet-connected devices used by pupils or on the school network.
 - Devices that join the school network temporarily (visitors, governors, contractors).
 - Remote access arrangements and cloud services used for teaching.
 - Guest Wi-Fi and any BYOD (bring your own device) arrangements – set out clear acceptable use and technical expectations.
- Edge cases and special topics
 - Generative AI: use in classrooms must meet DfE product safety expectations; filtering/monitoring must consider AI tools and how outputs are used. Staff must follow guidance for safe use of generative AI.
 - Use of school facilities by external groups: the school will ensure external users cannot exploit facilities or IT to spread extremist or harmful content and will apply the Prevent guidance when booking or permitting events.
 - Pupils with specific needs: filtering settings should not prevent access to required curriculum material for pupils with SEND; where necessary, the DSL and SENCo will agree reasonable adjustments.

Records and documentation

- The school will maintain:
 - a decision log of items explicitly blocked/allowed with rationale;
 - evidence of checks on all internet-connected devices and locations;

- monitoring logs and records of safeguarding actions taken following alerts (retained under the school's data-retention policy); and

Data protection and confidentiality

- The school will process monitoring data in accordance with data protection law. When sharing personal data internally or externally (for example Prevent referrals), staff will consider lawful basis and follow the school's information-sharing protocols and the Information Commissioner's Office guidance.

Training and staff awareness

- All staff will receive online safety training which includes: the school's filtering and monitoring approach, how to interpret and respond to alerts, and how to report technical or safeguarding concerns. New staff will be briefed on appointment.

Quick escalation flow for staff (short version for staff handbook)

- If you see or suspect a pupil has accessed harmful content: secure the device (if safe to do so), record what you observed, report immediately to the DSL, and preserve logs/screenshots if instructed.
- For technical failures: report to IT provider and SLT lead immediately.
- For curriculum activity likely to trigger filtering logs: tell the SLT lead/IT provider ahead of the lesson and record the rationale.

Sources and further reading

- Keeping Children Safe in Education (KCSIE) – Statutory guidance (July 2026).
- DfE – Filtering and monitoring standards; Plan technology for your school service.
- Maintained schools: governance guide (July 2026) – digital and technology infrastructure section.
- Prevent duty guidance: for England and Wales (March 2024) – education sector guidance.
- UK Safer Internet Centre and SWGfL resources (for practical checks and provider lists).