Internet Filtering and Monitoring Policy

RESPONSIBLE DIRECTOR
Operations Director

RATIFIED BY TRUST
June 2026

REVIEW DATE
June 2027

1 Aims

This policy aims to guide schools to be able to set the internet filtering systems so they are appropriate to the school and ensure that there are adequate monitoring procedures in place.

2 Legislation and Guidance

The policy Reflects the statutory requirement for governing bodies and proprietors to meet the DFE standards for filtering and monitoring as set out in Keeping Children Safe in Education 2023. This policy will be followed by all KST schools.

3 Definitions

Filtering systems: block access to harmful internet sites and content to protect children on school premises.

Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school devices. Schools should be alerted to any concerning content so they can intervene and respond.

4 Responsibilities

The day to day management of filtering is shared by the DSL, the operations team and the IT service provider. In order for a school's filtering and monitoring systems to be effective all parties need to work closely together to:

- Procure systems
- Identify risk
- Carry out reviews
- Carry out checks
- Complete corrective actions.

The DSL is responsible for overseeing and acting on:

- Filtering and monitoring reports
- Responding to safeguarding concerns
- Ensuring there are checks to filtering and monitoring systems
- Reporting to the local governing body on the efficacy of the systems and reporting the number and nature of serious incidents that require further investigation.
- Following up with pupils on the circumstances of particular incidents and recommending corrective action or consequences for the pupil

The Operations Director/Manager is responsible for:

- Buying the filtering and monitoring system that are used in schools
- Ensuring that documentation is in place that manages what is blocked
- Instructing IT service providers to change settings
- Ensuring the monitoring procedures are robust
- Ensuring the DSL has access to the reports of incidents involving pupils.
- Ensuring that significant changes to the filtering and monitoring system and process have been passed through an appropriate change impact assessment with key stakeholders (e.g. Headteachers and DSLs)

IT service provider is responsible for:

- Maintaining the filtering and monitoring systems are robust and secure 24/7
- Managing the update of all filtering and monitoring systems
- Providing filtering and monitoring reports as requested
- Checking the system or completing actions following any corrective actions requested.

The Head teacher is responsible for:

- Reviewing the effectiveness of the provision, making sure that serious incidents/breaches are urgently picked up, acted on and outcomes are recorded on CPOMS
- Requesting changes to the filtering criteria
- Working with the Operations team to complete and sign-off a change impact report
- Overseeing reports and ensuring the DSL is responding to issues
- Follow up with staff any attempted access of inappropriate material
- Making sure the staff:
  - Understand their role
  - Are trained appropriately
  - Follow policies, processes and procedures
  - Act on reports and concerns.

All staff should be clear on:

- The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training.
- How 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 a failure in the software or an 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 LGB has overall strategic responsibility for ensuring there is robust filtering and monitoring in place that meets the DFE standards. They will need assurance that the school is meeting the standards and they need to be aware of the filtering and monitoring arrangements through the receipt of regular reports.

5 Filtering Arrangements

Filtering should cover the following categories:

- Abuse
- Adult Content
- Bullying
- Criminal Activity
- Radicalisation
- Substance Abuse
- Suicide

Each school needs appropriate filtering arrangements which should cover all technology that accesses the school internet network. This should include staff devices, pupil devices, personal laptops and personal mobile phones. In essence, any access to the internet using the school internet link (Wi-Fi and cable) is filtered.

The sensitivity of the filtering arrangements is different for each school e.g. a primary school will filter at a more sensitive level than a secondary school, or a Key Stage 3 or 4 pupil could have different filters applied to a Key Stage 5 student. Each school needs to work with the operations/IT teams to ensure that the appropriate level of filtering is in place.

Staff will need to have the appropriate level of internet access to enable them to prepare lessons and access material for teaching. These levels of access will need to be determined with the school so that staff are not necessarily hampered in their work.

Filtering must be able to stop access to sites that are inappropriate for children and be able to stop search engines producing inappropriate content e.g. image search.

Filtering needs to be able to allow access to approved platforms but restrict inappropriate content on that platform e.g. You Tube is an authorised platform but holds content that will be inappropriate, google image search is a useful tool but can display content that is inappropriate.

Filtering systems are not currently the same across the Trust schools due to previous procurement and that there are different IT contractors. IT policy is to harmonise systems where possible. However, all systems need to be compliant to this policy.

Filtering is limited to devices that access the school's internet, we are not able to filter personal devices that access the internet by a person's 4G/5G mobile account.

6 Monitoring Arrangements

Active Pupil Monitoring

Trust policy is to implement 'active monitoring' of pupil computer interactions. Software is installed on every student/pupil device that is owned by the school/trust (both pc and iPad). When a pupil types in a banned or concerning search term e.g. "how do I commit suicide" it will automatically take a screen shot and document the incident. This information will be sent to the DSL who can inspect the incident and decide the appropriate course of action.

Active Staff and Visitor Monitoring

Trust policy is that the Headteacher at each school can request that staff monitoring is turned on. The Headteacher can inspect their staff's computer interactions. It is not recommended that the alert function is turned on, although depending on the software functionality this can be arranged if the situation warranted it. Staff should be informed that any attempted access to banned sites will be logged and monitored, this includes interactions at home.

7 Reporting

The following reporting arrangements should be in place across all schools in the trust.

- Pupil attempted access to concerning material is immediately reported to the DSL
- Concerning staff and visitor attempted access is reported to the DSL/Headteacher on a monthly basis
- Summary reports are made by the headteacher/ DSL to the LGB on a termly basis
- Any changes to the filtering system criteria should be reported to the operations team by the IT contractor, changes requested by the school need to be approved by the head teacher.

Staff should raise an IT ticket if sites that are blocked need to be unblocked, this can take up to 24 hours for the change to take effect.

8 Checks

The following checks need to be made

- IT need to check that software updates are implemented immediately.
- IT need to check that the software is working appropriately on a half termly basis.
- DSL's and Headteachers should independently perform a review of whether the filtering and monitoring systems are being effective on a termly basis and immediately report any problems to Operations.
- The safeguarding governor should check school compliance with the policy as part of their regular safeguarding review.
- Operations should report to the KST board on the implementation and effectiveness of the policy as part of their regular reporting.

Palingswick House
241 King Street
Hammersmith
London W6 9LP
T 020 8600 0670
E contactkst@ks-t.org

www.knowledgeschoolstrust.org