

Monitoring and Filtering arrangements. September 2025.

Rationale

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

Responsibilities

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

We have identified and assigned:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers

We are aware that it must be possible to make prompt changes to our provision.

Technical requirements to meet the standard

The senior leadership team are responsible for:

- procuring filtering and monitoring systems, we have done this through LGfL
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Our IT technician is an external service provider (Datasol.)

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of our setting. We work with our filtering or monitoring providers for system specific training and support.

Meeting the standards.

The DSL takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns

- checks to filtering and monitoring systems

The IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider works with the senior leadership team and DSL to:

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

For filtering and monitoring to be effective it must meet the needs of our pupils and staff, and reflect our specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of our school or college, we will review our filtering and monitoring provision, at least annually using the LGfL template.

Additional checks to filtering and monitoring will be informed by the review process so that governing board has assurance that systems are working effectively and meeting safeguarding obligations.

The governing board has overall strategic responsibility for meeting this standard. They will make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review will be recorded for reference and made available to those entitled to inspect that information.

Technical requirements to meet the standard

A review of filtering and monitoring will be carried out to identify our current provision, any gaps, and the specific needs of our pupils and staff.

We will consider:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what our filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements, for example, our RHSE and PSHE curriculum
- the specific use of our chosen technologies,
- what related safeguarding or technology policies we have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff

- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

There are templates and advice in the reviewing online safety section of [Keeping children safe in education](#).

Checks to our filtering provision need to be completed and recorded as part of our filtering and monitoring review process. How often the checks take place should be based on local context, the risks highlighted in our filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems we will make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

We will keep a log of our checks so they can be reviewed. We will record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

We will make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

We will use South West Grid for Learning's (SWGfL) [testing tool](#) to check that our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

Our filtering system will block harmful and inappropriate content, without unreasonably impacting teaching and learning.

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

No filtering system can be 100% effective. We will endeavour to understand the coverage of our filtering system, the limitations it has, and mitigate accordingly to minimise harm and meet our statutory requirements in [Keeping children safe in education](#) (KCSIE) and the [Prevent duty](#).

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

Our governing board will support the senior leadership team to procure and set up systems which meet standards and the risk profile of the school or college.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. We will ask our filtering provider for system specific training and support.

Technical requirements to meet the standards

We will ensure our filtering provider is:

- a member of [Internet Watch Foundation](#) (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Our filtering provision is procured with a broadband service, and we understand we need to ensure it meets the needs of our school.

Our filtering system should be operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Our filtering system should:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If our users access content in this way, we should get confirmation from our provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

Our filtering systems will allow us to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Schools and colleges need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. [A DPIA template](#) is available from the ICO.

[The DfE data protection toolkit](#) includes guidance on privacy notices and DPIAs.

The UK Safer Internet Centre has guidance on establishing [appropriate filtering](#).

Our senior leadership team may decide to enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for our users on top of the filtering service.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which 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

Dependencies to the standard

We will regularly check that we meet:

- [Broadband internet standards](#)
- [Cyber security standards](#)

We will have effective monitoring strategies that meet the safeguarding needs of our school or college.

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows us to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Our monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Governing boards should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure their knowledge is current. You may need to ask our monitoring system provider for system specific training and support.

Technical requirements to meet the standard

Governing boards should support the senior leadership team to review the effectiveness of our monitoring strategies and reporting process. We will ensure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding

nature. It should be clear to all staff how to deal with these incidents and who should lead on any actions.

The UK Safer Internet Centre has guidance for schools and colleges on establishing [appropriate monitoring](#).

Device monitoring can be managed by IT staff or third party providers, who need to:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

We will make sure that:

- monitoring data is received in a format that our staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

If mobile or app technologies are used then you should apply a technical monitoring system to the devices, as our filtering system might not pick up mobile or app content.

In the online safety section of [Keeping children safe in education](#) there is guidance on the 4 areas of risk that users may experience when online. Our monitoring provision should identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

School and college monitoring procedures need to be reflected in our Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. [A DPIA template](#) is available from the ICO.

[The DfE data protection toolkit](#) includes guidance on privacy notices and DPIAs.

Date of Policy: November 2025.

Review date: November 2026.

Approved by: Full Governors 18th November 2025.

Signed

Chair of Governors

Headteacher