DSAT Filtering and Monitoring Policy 2023
Changes to 'Keeping Children Safe in Education' (KCSIE)

In March 2023, the DfE further updated the guidance in KCSIE to include three new sections:

- Cloud Solution standards
- Servers and Storage standards
- Filtering and Monitoring standards

In this document we will summarise these changes and how we go about meeting these standards at DSAT.

1. You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

The importance of meeting the standard – what the guidance states

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.

Requirements to meet the standard

The trust and senior leadership team in school are responsible for:

- Procuring filtering and monitoring systems (Dan and Nevine)
- Documenting decisions on what is blocked or allowed and why (Dan)
- Reviewing the effectiveness of your provision (Dan and Nevine)
- Overseeing reports (Dan, Nevine and the Leadership Team)

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 should work closely with the DSAT Central Team (Dan and Nevine), the designated safeguarding lead (DSL) and IT support in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT support to be effective. The DSL should work closely together with DSAT's IT support team to meet the needs of your setting.

The DSL should take 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 (Dan and Nevine do this termly)

DSAT IT support should have technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems

DSAT IT support and Head of Business and Operations should work with the senior leadership team and DSL to:

- Procure systems
- Identify risk
- Carry out reviews
- Carry out checks

2. You should review your filtering and monitoring provision at least annually

The importance of meeting the standard – what the guidance states

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

To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision, at least annually.

Additional checks to filtering and monitoring need to be informed by the review process so that we have assurance that systems are working effectively and meeting safeguarding obligations.

Requirements to meet the standard

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

You need to understand:

- The risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- What your filtering system currently blocks or allows and why
- Any outside safeguarding influences, such as county lines
- Any relevant safeguarding reports
- The digital resilience of your pupils
- Teaching requirements, for example, your RHSE and PSHE curriculum
- The specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- What related safeguarding or technology policies you have in place
- What checks are currently taking place and how resulting actions are handled

To make your filtering and monitoring provision effective, your review should 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 should 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

Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your 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 you should 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

You should keep a log of your checks so they can be reviewed. You should record:
- When the checks took place
- Who did the check
- What they tested or checked
- Resulting actions

You should 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

You can use South West Grid for Learning's (SWGfL) testing tool to check that your filtering system is blocking access to (*https://swgfl.org.uk/services/test-filtering/*):
- Illegal child sexual abuse material
- Unlawful terrorist content
- Adult content

3. Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

The importance of meeting the standard – what the guidance states

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. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your 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.

Requirements to meet the standard

Make sure your 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)

The Smoothwall devices in DSAT schools comply with all these standards.

Your filtering systems should allow you 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.

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

4. You should have effective monitoring strategies that meet the safeguarding needs of your school or college

The importance of meeting the standard – what the guidance states

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 you 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.

Your 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

THE DIOCESE OF SHEFFIELD ACADEMIES TRUST

Requirements to meet the standard

DSAT will support the senior leadership team to review the effectiveness of your monitoring strategies and reporting process. Make sure 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.

Device monitoring can be managed by DSAT IT support, 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

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.

Additional Online Resources

DfE Data Protection Toolkit: https://www.gov.uk/guidance/data-protection-in-schools

Internet Watch Foundation: https://www.iwf.org.uk

DfE Data Protection Toolkit: https://www.gov.uk/guidance/data-protection-in-schools

UK Safer Internet Centre guidance on establishing appropriate filtering and monitoring: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

DfE Meeting digital and technology standards in schools and colleges: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges