schools broadband™

Filtering & Monitoring Standards for Schools

Updates to DfE Filtering & Monitoring Standards
And How Your School Can Meet Them

IWF Internet Watch Foundation

RIPE NCC Member

besa BRITISH EDUCATIONAL SUPPLIERS ASSOCIATION

schools broadband

About This Guide

The Department for Education's Filtering and Monitoring Standards for Schools and Colleges were updated in October 2024 to reflect the changing digital landscape and provide greater clarity on some key issues.

This guide has been created to help schools, colleges and MATs understand clearly how they should implement filtering and monitoring in their settings. It outlines the standards that organisations should already be meeting, a summary of the changes, and how to respond accordingly.

It is essential reading for: SLTs, DSLs, IT staff, headteachers, governors, proprietors and anyone with a responsibility for or interest in safeguarding children and young people.

Filtering & Monitoring - What's the Difference?

Filtering
Web filtering is a preventative measure that blocks access to harmful, inappropriate, or illegal online content by analysing and restricting specific websites, links, and media. It ensures users are shielded from exposure to unsafe material before they encounter it.

Monitoring
Monitoring, on the other hand, is a reactive solution that tracks user activity on devices without blocking access. It generates reports or real-time alerts based on concerning behaviour or interactions, such as bullying or accessing harmful content, allowing staff to intervene as needed.

Together, these solutions provide a comprehensive approach to safeguarding users online, balancing prevention with the ability to respond to emerging risks.

Standard 1

Identify and assign roles and responsibilities to manage your filtering and monitoring systems.

Update
"Illegal" has been added to the list of material that filtering and monitoring should safeguard students and staff from.

Explained
As well as inappropriate and harmful content, filtering and monitoring should protect users from illegal content, such as material promoting terrorism.

Update
Clarification has been provided to confirm that DSLs and IT support should work together to deliver and maintain filtering and monitoring, with support and checks provided by governors and senior leadership teams.

Explained
This clarifies what previously referred to the importance of "the right people" working together.

Update
More information has been included on the responsibilities of DSLs in relation to filtering and monitoring.

Explained
In addition to checking relevant filtering and monitoring reports, the guidelines state that DSLs are also responsible for:

- Responding to safeguarding concerns identified by filtering and monitoring
- Assuring governors that filtering and monitoring systems are effective and regularly assessed
- Communicating relevant policies to all users, parents and carers

schools broadband™

Standard 2

Review your filtering and monitoring provision at least annually

Update
Schools are to conduct reviews of filtering and monitoring provisions at least "once every academic year."

Explained
Previously guidelines stated reviews should be carried out "at least annually."

Update
Reviews of filtering and monitoring provisions should take into account "technical limitations, for example, whether your solution can filter real-time content."

Explained
There are various types of web filters available to schools, with differing abilities. Schools should acknowledge risks that may result from the limited abilities of their solutions.

Update
Reviewing filtering and monitoring provisions now requires an understanding of how the school uses "generative AI tools."

Explained
This update is a response to the fact that schools may now use generative AI tools. This can pose a challenge to filtering and monitoring systems. For example, web filters that only inspect URLs may struggle to assess AI content. This can leave students exposed to the potentially harmful content that AI can produce.

Update
"Following system or equipment changes, you should seek assurance that all filtering and monitoring solutions will continue to work on all school-managed devices."

Explained
Introducing new devices can impact the ability of filtering and monitoring systems to work effectively. Technical limitations may occur if devices and safeguarding software are incompatible or not set up correctly.

Schools and colleges should assess that suitable levels of filtering and monitoring can still be achieved with any new equipment or systems that are introduced.

Update
The list of instances that require a review of filtering and monitoring systems has been expanded to include when:

- Major software updates occur
- Changes are made to the technical configuration of the network and devices

Explained
These assessments should take place in addition to those carried out once every academic year, and any risks that are identified should be investigated and addressed, either by adjusting device settings or reviewing the suitability of filtering and monitoring provisions.

Schools are also advised to "consider your student risk profile when deciding whether to continue using the devices in question."

Find out more. Call or email:
01133 222 333
info@schoolsbroadband.co.uk

Standard 3

Filtering systems should block harmful and inappropriate content, without unreasonably impacting teaching and learning

Update
The importance of having different risk profiles set up on filtering systems is emphasised.

Explained
Filtering levels need to be adjusted for different users, based on factors like age and status. Student and staff profiles should be in place to provide differing levels of access to online content. Schools should consider the different maturity levels and learning requirements of year groups when implementing filter settings.

Update
Clarification is provided on expectations for filtering blocklists.

Explained
Schools must make sure that their filtering solutions include the blocklists provided by The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU). These two blocklists cannot be disabled or have items removed from them by the provider or anyone at the school. If items are added to the blocklist, schools should "make sure that any additions do not disrupt or affect teaching and learning."

Update
Clarification provided on expectations for schools implementing a bring your own device (BYOD) policy.

Explained
Any devices that are not school managed "should be on a separate virtual network." This may involve IT support changing the setup of core networking equipment. Schools that already implement a BYOD policy may need to review their guidelines in light of this change. IT support may need to check devices are compatible with existing filtering and monitoring provisions before allowing their use on school premises.

Update
The list of requirements for filtering systems has been expanded to include the ability to:

- Identify and block portable wifi devices
- Block end-to-end encryption methods

Explained
Privacy features like end-to-end encryption are an increasingly popular tactic of filter avoidance. Schools are instructed to check with providers that their filtering systems are able to address these challenges. If in any doubt, "ask your IT support or filtering provider to block these technologies at a system level."

Providers also need to confirm that "networks and clients are appropriately configured", taking into account varying versions of firewalls, browsers, operating systems and software.

Standard 3 Cont.

Filtering systems should block harmful and inappropriate content, without unreasonably impacting teaching and learning

Update
The descriptions of devices and users to whom filtering should be applied has been updated.

Explained
Filtering should be applied to: "school or college-managed devices, including those taken off-site; unmanaged devices under a bring your own device (BYOD) scheme; [and] guests who have access to the school internet."

Filtering policies should be clearly defined for each of these scenarios and communicated across the school community.

Update
In addition to having a filtering solution in place, schools/colleges are now required to have 'safe-search' turned on, or use child-friendly search engines.

Explained
The safe-search engine must be locked into the chosen browser, so that it cannot be changed. Users are also prohibited from downloading additional browsers or unauthorised plugins that can circumvent safe-search settings.

Find out more. Call or email:
01133 222 333
info@schoolsbroadband.co.uk

Standard 4

Have effective monitoring strategies that meet the safeguarding needs of your school or college

Update
The guidance confirms that monitoring solutions can be technical or manual, and explains the factors to consider when selecting effective monitoring strategies for your setting.

Explained
Decisions on appropriate monitoring should take into account:

- Student ages
- Student risk profiles
- Whether screens are easy to see
- The number of devices in use
- Whether devices are used outside of school

Update
A minimum target for monitoring reports is provided.

Explained
Schools and colleges are advised that their monitoring strategies should at the very least "include weekly monitoring reports highlighting incidents."

Update
Schools are required to inform "everyone using your network" that filtering and monitoring processes are in place.

Explained
The guidelines suggest that this could be achieved with "a message each time they log in."

Technical monitoring systems in particular should "notify users that the device is being monitored."

Organisations can include the rationale behind monitoring in related policies, such as their acceptable use policy. These policies should also be shared with parents and any visitors to the school or college.

Update
School staff should perform in-person monitoring when supervising students who are using devices, even in settings where technical monitoring solutions are implemented.

Explained
If a school only conducts in-person monitoring, and risks are identified during reviews, they should consider having "additional technical monitoring solutions in place".

Update
A new section has been added that expands on previous descriptions of how monitoring plans should make clear to staff the way monitoring incidents are to be dealt with.

Explained
The plan should cover:

- How to deal with incidents
- Who should lead on any actions
- When incidents should be acted on (this should be in line with your school's policy – see standard 1 for further guidance)

To help measure the effectiveness of filtering and monitoring strategies, "there should be a documented process for recording incidents that includes what action was taken and the outcomes."

Does your school meet the standards?

The recent updates to the DfE's standards on Filtering and Monitoring emphasise the critical importance of safeguarding technology in schools. Ensuring your systems meet these requirements is essential for protecting students and remaining compliant. If you're unsure whether your school meets the latest standards or would like expert advice on filtering and monitoring solutions, our team is here to help.

Get in touch to ensure your school's safeguarding solutions are up to standard.
01133 222 333 | info@schoolsbroadband.co.uk | www.schoolsbroadband.co.uk

About Schools Broadband

Schools Broadband is a leading provider of connectivity, safeguarding, and security solutions designed for education. Since 2007, we've been committed to delivering reliable, secure, and cost-effective digital infrastructure to schools, Multi-Academy Trusts, and Local Authorities, ensuring full compliance with regulatory requirements.

Our smarter cloud-hosted technology raises standards without the need for expensive equipment. As a multiple ISPA Award winner for Best Security and Cloud Services, we offer some of the most advanced and affordable security solutions available to schools.

We keep schools safe with Prevent Duty and KCSiE-compliant filtering and monitoring, enhanced by our unique analytics, telemetry, and reporting systems. These tools provide DSLs and network managers with valuable insights into online behaviour, safeguarding concerns, and network usage - helping schools operate smarter and safer than ever.

Find out more. Call or email:

01133 222 333
info@schoolsbroadband.co.uk
www.schoolsbroadband.co.uk