WARRINGTON
Borough Council

LA provided solution for Web Filtering and Monitoring

Over the past few months, we have received questions from several schools and academies relating to the filtering and monitoring solution the LA provides to schools, and how it meets the standards as set out by the DFE.

To provide transparent guidance and assurance the LA have provided notes on the current solution the LA provide to schools as it is installed and configured today. This is provided with additional guidance schools and academies need to be aware of. All LA notes are in italics only and preceded by the heading "LA Guidance" for clarity

The DFE has produced this set of standards to help schools understand what they should be looking at with relation to Filtering and Monitoring, with the key aim to ensure that schools, governors, and management teams understand what is needed and why. The DFE do not publish a list of approved or sanctioned solutions to meet these standards.

For reference the detail that now follows is an extract from the following website: -

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

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

Why this standard is important

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

No filtering system can be 100% effective. You need to understand:

- your filtering system's coverage
- any limitations

You should mitigate against these limitations to minimise harm and meet your statutory duties in the filtering and monitoring section of Keeping children safe in education and the Prevent duty guidance: England and Wales (2023)

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 or college administration
- restrict students from learning how to assess and manage risk themselves

How to meet the standard

Governing bodies and proprietors need to support the senior leadership team (SLT) to procure and set up systems which meet this standard and satisfy your school or college risk profile. This may need to be different for different user types, year groups and subjects.

Your filtering system should not have a blanket filtering profile for all users. As a minimum, student and staff profiles should be in place to provide differing levels of access to online content.

LA Guidance

The way the LA provided solution is deployed means that each individual school/academy receives one profile. This blanket profile affects all traffic utilising the LA provided circuit.

Filtering system management requires specialist knowledge from both safeguarding and IT support to be effective. You may need to ask your filtering provider for system specific training and support.

Technical requirements to meet the standard

The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) provide lists of illegal websites that filtering providers can block as part of their service, known as blocklists. Schools and colleges must make sure these blocklists are included with their filtering solutions. Your school or college should not be able to disable these blocklists or remove items from them.

Also make sure that your filtering provider is:

- a member of IWF
- signed up to CTIRU
- regularly updating blocklists based on information from IWF and CTIRU

LA Guidance

The LA provided solution is a member of the IWF and utilises block lists from both the IWF and CTIRU which are transparently updated.

Some schools and colleges may want to block additional, inappropriate content that their filtering system does not automatically block. Your system should allow you to add this content locally. Any additions should not disrupt or affect teaching and learning.

LA Guidance

The LA solution provides allowance for each school/academy to have their own explicit block and allow sites, for example some schools/academies can access Facebook, whilst others cannot.

Regardless of solution implemented it remains the direct responsibility of the school/academy to understand what they are explicitly allowing or blocking and to be able to provide justification for it if challenged by parents, governors, inspectors etc.

Your filtering system should be active, up to date and applied to all:

- school or college-managed devices, including those taken off-site
- unmanaged devices under a bring your own device (BYOD) scheme
- guests who have access to the school internet

LA Guidance

The filtering system as provided by the LA is applied at the internet circuit level. All traffic utilising the LA provided internet circuit is filtered according to the profile and explicit rules set for that school/academy.

Devices which are taken away from the school/academy and/or allowed to use an alternate internet circuit are not protected by the LA provided solution unless a 3rd party VPN, routing traffic from the device back to the school and then out onto the internet via the schools network, has been setup and deployed.

The physical units providing the filtering are additionally kept up to date with BIOS and firmware twice a year by default, with any important/critical security-based BIOS and firmware updates applied as soon as notified.

Devices that are not school or college-managed, should be on a separate virtual network. Check with your provider to find out whether your filtering system:

- identifies and appropriately filters all internet feeds, including any backup connections and portable wifi devices
- is appropriate for the age and ability of the users
- is suitable for educational settings
- identifies multilingual web content, images, common misspellings and abbreviations
- provides alerts when web content of concern has been blocked
- blocks technologies and techniques that allow users to get around the filtering, such as VPNs, proxy services and end-to-end encryption methods

If you are unsure about how to do this, ask your IT support or filtering provider to block these technologies at a system level. Also ask them to make sure that networks and clients are appropriately configured, this covers everything from firewalls and browsers to operating systems and software.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your 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.

<u>LA Guidance</u>

The LA solution filters all and any traffic on the LA provided circuit, mobile devices using 3/4/5 G mobile or alternate networks are not covered by the solution.

The solution does block technologies and techniques like VPN and proxy solutions

If a blocked website is attempted to be accessed staff/learners are presented with an alert, informing them that the website they have tried to access is blocked and informs them why.

The solution is global and language agnostic, If a website is mis-spelled then the web request is treated the same as any other web request and filtered accordingly.

The LA solution does not directly filter images. Images are instead filtered in one of two ways.

- *Google safe search is enforced as long as the school/academy is utilising the correct DNS entries the LA provide. This provides the first tier of safety.Web domain.*
- *If the image is found on a website which is itself blocked either explicitly or via detection from the block lists provided by IWV or CTRIU, then it will also be filtered out.*

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 SLT or the designated safeguarding lead.

Your filtering systems should allow you to identify, as a minimum:

- 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

LA Guidance

The LA provided solution can identify IP address of devices alongside time/date of attempted access. The solution also captures the type of content or specific website that an attempt was made to visit.

IP address detection requires the school to allow these IP Addresses to be visible from the Internet circuit the LA provides and not obfuscated or behind a NAT technology.

Schools and colleges will need to conduct their own data protection impact assessments (DPIAs) and review the privacy notices of third-party providers. A DPIA template is available from the Information Commissioner’s Office (ICO).

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Search engines used should have safe search enabled by default, or use a child-friendly search engine, to provide an additional level of protection for your users in addition to the filtering service. Make sure that:

- your safe search engine is locked into your chosen browser and cannot be changed
- users cannot download additional browsers or unauthorised plugins

If the filtering provision is procured with a broadband service, ask your broadband provider how it meets these requirements.

LA Guidance

The LA solution enforces Google safe search; please note this is dependent upon the network or curriculum side of the network being configured to use the correct DNS entries.

The LA solution does not control the ability for end users to download additional browsers or unauthorised plugins onto curriculum devices, and the school/academy should speak directly with their curriculum support company for advice and guidance around this area.

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

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

LA Guidance

Please be aware that the term unsuitable used by the DFE is intentionally open to a level of interpretation, as unsuitable will differ from school to school and in some instances from year to year. It remains the responsibility of the school/academy to determine what unsuitable means in their specific environment.

Dependencies to the standard

Check that you meet:

- broadband internet standards
- cyber security standards

Further LA Guidance

Under the broadband internet standards dependencies the DFE state that schools/academies should be using full fibre connections that is an internet/broadband circuit that does not use copper connectivity beyond the physical building.

Schools/Academies can request a quote from the LA to upgrade their internet provision to meet this requirement.

The standards also states that schools/academies should have a backup internet feed and a resilient service to prevent service disruption.

The LA can provide quotes for geographically diverse circuits if required and assist with resilient network planning.

Under the Cyber security standards schools/academies need to understand and engage with IT specialists to ensure that key IT infrastructure is not insecurely exposed to the internet, and that the risk of data loss , with the potential for safeguarding, reputational and financial damage is as far as possible mitigated.

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

Why this standard is important

Monitoring user activity on school and college devices is an important part of providing a safe environment for students 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. There are both technical and manual solutions. Which solution your school or college uses will depend on your educational setting, including:

Monitoring user activity on school and college devices is an important part of providing a safe environment for students 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. There are both technical and manual solutions. Which solution your school or college uses will depend on your educational setting, including:

- student age
- student risk profile
- whether screens are easy to see
- number of devices in use
- whether devices are used off-site, for example, at home

For monitoring to be effective it must pick up incidents that are of concern urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

How to meet the standard

All staff should conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision. Some schools and colleges may decide to have additional technical monitoring solutions in place to reduce any risks identified during the review.

The designated safeguarding lead (DSL) is responsible for any safeguarding and child protection matters that are identified through monitoring.

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

Technical requirements to meet the standard

Your monitoring plan should include how you will monitor students when using school-managed devices connected to the internet. This could include:

- device monitoring using device management software
- in-person monitoring in the classroom
- network monitoring using log files of internet traffic and web access

As a minimum, your monitoring plan should include weekly monitoring reports highlighting incidents. It should also include immediate reports when an incident is classed as high-risk, for example, those of a malicious, technical or safeguarding nature.

LA Guidance

The LA provided solution only monitors internet/Web based traffic. It does not produce reports or alerts directly to the school/academy.

If the school/academy did, through other forms of monitoring, notice an issue, the LA could provide specific reporting based upon the time/date/IP Address of the device.

Make sure that everyone using your school's network knows that filtering and monitoring processes are in place. Technical monitoring systems should also notify users that the device is being monitored. This could be a message each time they log in.

Your monitoring plan should include how you communicate with staff about accepted ways of responding to incidents, including:

- how to deal with incidents
- who should lead on any actions

- when incidents should be acted on, in line with your school’s policy – read the first standard about filtering and monitoring roles and responsibilities to help with this

There should be a documented process for recording incidents that includes what action was taken and the outcomes. This will help you to understand the effectiveness of your filtering and monitoring plan.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.

Device monitoring can be managed by in-house or third-party IT support, who need to:

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

Make sure that:

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

LA Guidance

The LA provided solution does not monitor individual devices.

If mobile or app technologies are used then you should apply a technical monitoring system to the devices, as your 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.

Your 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 students
- report any safeguarding concerns to the DSL

School and college monitoring procedures need to be reflected in your acceptable use policy (AUP). Add them to 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. Visit the Information Commissioners Office website to download a DPIA template.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

LA Guidance

THE DFE standards for meeting digital and technology standards in schools and colleges is comprised of the following main areas

- *Filtering and Monitoring*
- *Broadband Internet standards*
- *Cyber security standards*

Schools and academies need to consider how they are meeting the standards listed overall which will be a blend of technology, process and manual based resources/strategies.

The DFE do not prescribe or endorse one specific solution to meet the standards, as there are many solutions available and it is the responsibility of the school/academy to ensure that the standards are being met in a way that is appropriate, and equally important can be justified if challenged.