INTERNET FILTERING AND MONITORING POLICY

2023-24

THE HAMMOND SCHOOL LTD., MANNINGS LANE, CHESTER, CH2 4ES

Telephone: 01244 305350 | Web: www.thehammondschool.co.uk | Email: contact@thehammondschool.co.uk

In keeping with the guidance publication, Keeping Children Safe in Education September 2023, The Hammond has a whole school policy regarding the safe usage of the internet. Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Filter content lists are regularly updated (via Sophos) and internet use is logged and monitored. There is a clear route for reporting and managing changes to the filtering system. Where we allow students and staff to bring their own devices, they are allowed internet access through the school network, filtering (via Sophos) will then be applied that is consistent with school practice.

- The school has provided differentiated user-level filtering through the use of Sophos devices. These allow for different filtering levels for different ages / stages and different groups of users – staff / pupils / students.
- Pupils / students will be made aware of the importance of filtering systems and the way in which the school's works upon their induction programme.
- Mobile devices that access the school internet connection will be subject to the same filtering standards as other devices on the school systems
- If a member or staff or a student has concerns regarding the accessible content, they can contact IT Support.
- If there are any concerns regarding a particular student or member of staff, the school can monitor their internet usage and lock their account until the matter is resolved.
- Any filtering issues are reported immediately to the filtering provider who then manage the filtering system remotely to resolve any problems.
- If the filtering system is compromised in any way, Sophos devices disallow connection to the source so there is no instance where students and staff can access the internet unfiltered.
- The measures above are carried out in accordance with Safeguarding and Prevent strategies in order to protect students from online threats presented by access to the internet.

The Hammond uses the Department for Education's published filtering and monitoring standards, which sets out the following:

- The Hammond should identify and assign roles and responsibilities to manage filtering and monitoring systems. This role is overseen by the Head of Student Support and the Director of Operations and Estates.
- The named staff meet the relevant member of the Board of Directors (Debbie Silcock and Anna Sutton) to review.
- The Hammond should review the filtering and monitoring provision at least annually. The Hammond's leaders (mentioned above) complete this exercise every August.
- The Hammond blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- The Hammond has effective monitoring strategies in place that meet safeguarding needs through the above.

- The Hammond's Safeguarding Board committee will include discussion of the above in subcommittee meetings from September 2023.

Filtering and monitoring standards for schools and colleges (following advice from KCSIE 2023)

The Hammond identifies and assigns roles and responsibilities to manage your filtering and monitoring systems

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.

How to meet the standard

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

To do this, they should identify and assign:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met – this is the Director of Operations and Estates and the Head of Student Support. These SLT members are responsible for strategic and operational oversight, as well as responding to need.
- the roles and responsibilities of staff and third parties, for example, external service providers - the named staff oversee the work and the training of The Hammond's external IT provider

The named staff are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your 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 Directors, the designated safeguarding lead (DSL) and IT service providers 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 staff to be effective. The DSL should work closely together with IT service providers 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

The IT service provider should have 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 should work with the senior leadership team and DSL to:

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

The Hammond reviews the filtering and monitoring provision at least annually

To understand and evaluate the changing needs and potential risks The Hammond, we review filtering and monitoring provision, at least annually.

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

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

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

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

The Hammond understands:

- the risk profile of pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the 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, the 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

There are templates and advice in the reviewing online safety section of Keeping children safe in education.

Checks to the filtering provision need to be completed and recorded as part of the 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:

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

Your filtering system should 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 need to understand the coverage of the 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

The Board of Directors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.

Technical 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)

If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.

Your 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

Your 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 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.

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.

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

Schools and colleges 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.

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

The Board of Directors may decide to enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for your 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

Check that you meet:

- Broadband internet standards
- Cyber security standards

You should have effective monitoring strategies that meet the safeguarding needs of your school

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 Board of Directors 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 your monitoring system provider for system specific training and support.

Governing bodies and proprietors should 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.

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

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

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 pupils
- report any safeguarding concerns to the DSL

School and college monitoring procedures need to be reflected in your 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.

Statement regarding use of mobile technology

The Hammond is fully aware of the high-profile use of mobile technology, particularly access to 3G and 4G and 5G internet, in the world today. It is acknowledged that this plays a large part in the lives of our pupils and students and can have positive outcomes. However, there are some clear risks when children are able to go online.

The NSPCC state that 'the most effective filter is an educated child'. We work closely with pupils to educate them on safe use of the internet through dedicated lessons, form tutor time, PSHE drop-down days and assemblies. During the school day, the following precautions are aimed at reducing the possibility of pupils having difficulties:

- Year 7 - 11 pupils may not have a phone on site
- College students may have a phone on site and must adhere to the Mobile Devices Policy
- During evenings, in the boarding houses, children are allowed access to their mobile devices but these are removed at bed time and locked away by Houseparents.

To support boarders, the following information is provided to the parents of boarders through our boarding handbook:

The controls you've set up on your child's device and your home broadband won't apply if they use 3G, 4G, or 4G public WiFi or log on to a friend's connection instead. Public WiFi is often available when you're out and about. But it's not always secure and can allow children to search the internet free from controls.

Some venues and businesses offer family-friendly WiFi. When you see the family-friendly WiFi symbol it means that when you connect to the WiFi there are filters in place to stop children from seeing harmful content. Talk to your child and agree with them what they can and can't do online. And if they're visiting friends or family remember that they might not have the same controls set up.

For step-by-step guides on how to set up on how to parental controls on specific mobile and broadband networks please see the link below:

https://www.internetmatters.org/parental-controls/broadband-mobile/

Please also see Mobile Devices Policy and Child Protection and Safeguarding Policy.

Policy Details

This Page Should Not Be Published

Document Owner:	J ROSCOE
Document Input:	SLT
Document Sources:	DFE
First Created Date:	JULY 2022
Last Update Date:	AUGUST 2023
File Location of Original Policy:	SHAREPOINT

Approver	SAFEGUARDING AND BOARDING COMMITTEE
Role	BOARD OF DIRECTORS
Last Approval Date	AUGUST 2023
Next Review Date	AUGUST 2024