Filtering & Monitoring Policy & Checklist for Online Safety

Document Owner:	B. Duffy
Approved By:	C-Suite
Queries to:	B. Duffy
Review Period:	3 years (or as relevant)

Contents

1. Introduction

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.

Keeping Children Safe in Education states, 'it is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.'

Part of this approach is to ensure that effective filtering and monitoring occur.

KSCiE now states that DSLs takes responsibility for F&M but this can only occur with IT support, so the day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective.

2. Aims and Objectives

Each academy within the Trust will have its own unique demands and use of the internet. However, all academies must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime. This policy is to give guidance to all academies to ensure that all systems are appropriately in place.

3. Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is also noted in KCSiE that, 'whilst it is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.'

It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. Academies use this flexibility to meet their learning needs.

4. Monitoring

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

5. Requirements of Online Filtering and Monitoring

All academies within the Trust must ensure that internet systems are robust and appropriate for use. Academies are required to ensure they meet the **'Digital and Technology Standards in Schools and Colleges'** (DfE 2023). Both DSL and IT Lead should be aware of this document.

The completion of the checklist in this document will evidence that each academy is fulfilling its duties in ensuring an effective monitoring and filtering system is in place. This will then ensure all leaders can consider any risk that both children and staff may encounter online.

The main aspects included in the standards are as follows:

a) **Identify and roles and responsibilities.**
b) **Review Filtering and Monitoring annually.**
c) **Filtering system should block out inappropriate content without unreasonably impacting teaching and learning.**
d) **Effective monitoring strategies should be in place that meet the safeguarding needs of the academy.**

a) Roles and Responsibilities

The Board of Trustees

The Board of Trustees has delegated the responsibility for monitoring the way in which online monitoring and filtering is implemented within each academy to the C-Suite and local governance procedures.

C-Suite

C-Suite is responsible for receiving reports when relevant of the overall effectiveness of safeguarding within academies. The Chief Infrastructure & Digital Officer will, together with the Director of Safeguarding & Compliance, make checks on the appropriateness of online filtering and monitoring systems in academies.

Local Governance

Local governance procedures will monitor the effectiveness of this policy within the academy, either through Progress Boards, Team around the School Boards and/or Academy Council/Local Advisory Boards. Each academy will determine in which part of local governance this sits.

Headteacher/Principal

Responsible for ensuring these standards are met and:

- will support the DSL with the implementation of this system
- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of provision
- overseeing reports

Ensure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns
- sign a Safeguarding Declaration each year which includes adherence to our Acceptable Use Policy.

DSL

Lead responsibility for safeguarding and online safety, which should include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems
- ensuring regular communications occur between academy and IT service provider, which may include training

DSL is responsible for completing the checklist (Annex A) in consultation with IT lead and then submitting as required.

Relevant IT Lead for academy's systems (this may be a staff technician or an external service provider.)

Responsibility for:

- maintaining filtering and monitoring technical systems
- ensuring system provides monitoring reports to safeguarding staff
- completing actions following concerns or checks to technical systems

Other staff

Other staff must ensure that they follow school policy with regard to appropriate use of the internet and that they use the school reporting mechanisms to alert leaders to any breaches in filtering and monitoring systems.

b) Review of Filtering and Monitoring System

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

Annex A in this document includes a checklist and can serve as the record that the review has occurred including being used as the report. This should be completed by 31st October each year and submitted/reported to Director of Safeguarding & Compliance at the Trust.

Additional ongoing checks to filtering and monitoring should also be performed when:

- a safeguarding risk is identified.
- there is a change in working practice, like remote access or BYOD (bring your own device).
- new technology is introduced.

The review should ensure academy leaders and governors understand:

- 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 filtering system currently blocks or allows and why.
- any outside safeguarding influences, such as county lines.
- any relevant safeguarding reports.
- the digital resilience of pupils.
- teaching requirements, for example, RHSE and PSHE curriculum.

- the specific use of chosen technologies, including Bring Your Own Device (BYOD).
- what related safeguarding or technology policies in place.
- what checks are currently taking place and how resulting actions are handled.

The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT Lead and involve the responsible governor.

c) Filtering System

The academy's filtering provider must be:

- 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, it needs to meet the needs of the relevant academy.

The system should:

- be operational and up to date.
- be applied to all:
  - users, including guest accounts.
  - school owned devices.
  - devices using the school broadband connection.
  - mobile and app use as well as web browser content.
- 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 (where appropriate system exists), 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.

The filtering systems should allow leaders 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.

Details of the academy's filtering systems is included in Annex A.

As stated in KCSiE, South West Grid for Learning (swgfl.org.uk) has created a tool to check whether an academy's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

d) Monitoring System

DfE Keeping Children Safe in Education requires schools to have "appropriate monitoring". DfE published Filtering and Monitoring standards for schools and colleges in March 2023. The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The academy must employ a monitoring strategy to ensure to minimise safeguarding risks on internet connected devices and may include some/all of those listed below. Technical monitoring systems do not stop unsafe activities on a device or online, so staff should:

- provide effective supervision, including physically monitoring watching screens of users, either actual screen or with device management software.
- take steps to maintain awareness of how devices are being used by pupils.
- report any safeguarding concerns to the DSL.
- use log files to monitor internet traffic and web access.
- ensure individual devices are monitored through software or third-party services.

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

- make sure monitoring systems are working as expected, including for any mobile or app technologies if used.
- provide reporting on pupil device activity.
- receive safeguarding training including online safety.
- record and report safeguarding concerns to the DSL.

Leaders and IT Lead must make sure that:

- monitoring data is received in a format that staff, especially safeguarding staff, can understand.
- users are identifiable to the academy, so concerns can be traced back to an individual, including guest accounts.

Academies 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.

Links with other policies

This policy will be monitored as part of the Trust's internal review and reviewed on a three-year cycle or as required by legislature changes.

This policy links to the following SET policies and procedures:

- Acceptable Use Policy
- Online Safety Policy
- Prevent Policy
- Staff Code of Conduct Policy
- Safeguarding & Child Protection Policy

In addition, the following are useful resources and sources of information both statutory and for guidance that academies may wish to access:

- Appropriate Filtering and Monitoring - UK Safer Internet Centre
- Data protection impact assessments | ICO
- Filtering and Monitoring | SWGfL
- Our Members (iwf.org.uk)
- Keeping children safe in education 2023 (publishing.service.gov.uk)
- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

"This policy has been equality impact assessed and we believe in line with the Equality Act 2010. It does not have an adverse effect on race, gender or disability equality."

Annex A: Academy Information and Standards Checklist

Academies must complete this checklist annually by 31st October and submit it to Trust Director of Safeguarding & Compliance (B. Duffy)

For 2023-24 only, that submission date is before 15th December 2023

Lead Adults	
DSL:	
IT Lead:	
Safeguarding AC Link:	

Filtering System	
Filtering Provider and System:	
Date Procured:	
Date last Reviewed:	
Monitoring System	
Monitoring Provider and System:	
Date Procured:	
Date last Reviewed:	

Questions:
Following completion of this checklist, are there questions DSLs/Academies have that they want support with or answers to? Please note below:

Academy Name:

Name of Staff completing Checklist:

Role:

		Yes/No	Comment
A	**Identify and assign <u>roles and responsibilities</u> to manage filtering and monitoring systems**		
1	Has academy leaders assigned this responsibility to appropriate staff to ensure the standards are met, and are each aware of their specific roles and responsibilities within this process? i.e. • DSL / IT Lead/Support / Academy Councillor		
2	Has academy leaders ensured that **all** staff: • understand their role. • are appropriately trained (inc. online / F&M / Cyber Security). • follow policies, processes and procedures for reporting. • act on reports and concerns.		
5	Does the IT Support/Lead and DSL communicate regularly ensuring procedures are in place and carry out reviews as appropriate?		

B	**Review filtering and monitoring provision at least annually**		
1	Do academy leaders/governing bodies ensure that filtering and monitoring provision is reviewed at least annually, to identify the current provision, any gaps, and the specific needs of your pupils and staff?		
2	Does the review cover all required elements (as a minimum) stated within this document in section 5b, c & d?		
3	Are report findings, i.e. this checklist, reported to relevant adults when completed: academy leaders / SET central / Academy Council		
4	Are findings used to inform improved practice?		
C	**Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning**		
1	Does the filtering system cover the relevant requirements listed in section 5c in this document?		
2	Is the filtering system checked regularly by safeguarding staff, e.g. using SWGfL tool or some other relevant method?		
3	Are academy leaders satisfied that whilst filtering system is in as required, it does not unreasonably impact on teaching and learning?		
4	Does the filtering system apply to mobile and app content?		
5	Does the academy systems meet with Cyber Security Standards?		
6	Is the filtering system configured to enforce compliance with the legal requirements outlined in the 'Illegal Content' section of the Appropriate Filtering guidelines provided by the UK Safer		

	Internet Centre? This includes ensuring the filtering applies to all devices, including pupil personal devices used on school wifi if used?		
D	**Have effective monitoring strategies that meet the safeguarding needs of academy**		
1	Does the monitoring system cover the relevant requirements listed in section 5d in this document?		
2	Does the monitoring system encompass reports from all devices, including pupils' academy iPads both on and offsite?		
3	Does the monitoring system ensure that urgent incidents, whether of a malicious, technical, or safeguarding nature are picked up same day (unless the incident occurs in the evening which should be addressed the next day.)?		
4	Has a data protection impact assessment (DPIA) been completed?		

Shaw Education Trust

Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
ST7 4DL

Twitter	@ShawEduTrust
LinkedIn	@ShawEducationTrust
Call	01782 948259
Email	info@shaw-education.org.uk
Visit	shaw-education.org.uk

Pupil & people centred

Act with integrity

Be innovative

Be best in class

Be accountable