



Monitoring & Filtering Policy

Policy Date: September 2025

Review Date: September 2027

Document History

Version	Status		Date	Author	Summary Changes
V1			Aug 24	M Sethi	
V2			Sep 25	M Sethi	Changes to roles and responsibilities
V3			Sep 26	S Clark	Added roles

Contents

1. Introduction
2. Aims and Objectives
3. Filtering
4. Monitoring
5. Requirements of Online Filtering & Monitoring, i.e. 'STANDARDS'
 - a) Roles & responsibilities
 - b) Review F&M 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.
6. Links with other Policies
7. Annex A: Academy Checklist for submission

1. Introduction

Schools, colleges and academy's should provide a safe environment to learn and work, including when online. Filtering and monitoring are both crucial aspects of safeguarding pupils and staff from potentially harmful and inappropriate online content.

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 involves ensuring that effective filtering and monitoring are in place.

KSCiE now states that DSLs take 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

Lumen Academy will have its own unique demands and use of the internet and will ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime.

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. Lumen Academy use this flexibility to meet their learning needs.

4. Monitoring

Monitoring user activity on Academy 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 Academy 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.

4

5. Requirements of Online Filtering and Monitoring

Lumen Academy ensures that internet systems are robust and appropriate for use. Lumen Academy ensures we meet the 'Digital and Technology Standards in Schools and Colleges' (DfE 2023). The principal, DSL, DDSL and the IT support team are aware of this document.

The main aspects included in the standards are as follows:

- a) Identify 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 principal has the responsibility for monitoring the way in which online monitoring and filtering is implemented within Academy. The DSL and the principal, together make checks on the appropriateness of online filtering and monitoring systems in the Academy. The DDSL is also responsible to assist the DSL.

The principal is 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 Acceptable Use Policy.

DSL is responsible 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,

Relevant IT team 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 Academy's policy regarding appropriate use of the internet and that they use the Academy's 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 Academy should review filtering and monitoring provision, at least annually.

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 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 team members

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)

The system should:

- be operational and up to date.
- be applied to all:
 - users, including guest accounts.
 - Academy owned devices.
 - devices using the Academy's 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.

6

- 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.

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 and/or DDSL.
- use log files to monitor internet traffic and web access.
- ensure individual devices are monitored through software or third-party services.

Device monitoring is managed by the principal, 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 and/or DDSL.

Leaders and IT team 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.

7

Links with other policies

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

This policy links to the following policies and procedures:

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

Reviewed By: Summer Clak September 2026

Next Review Date: September 2027

Approved by Director: 1st September 2026

Signed:



Monika Sethi
Principal and Director

8