At Knights Enham Schools we provide…

Inclusive and ambitious learning experiences where our school community feels safe and motivated to achieve their best.

'Together We Achieve'

Filtering and Monitoring POLICY

Approved: Sept 2024

Date of next review: Sept 2025

1. Introduction

Schools in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales).
Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”.
The use of technology has become a significant component of many safeguarding issues. With child sexual exploitation, radicalization and sexual predation, technology often provides the platform that facilitates harm. Our aim is to protect and educate the whole school community in our use of technology and to establish mechanisms to identify, intervene in and escalate any incident where appropriate.
The Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or college’s IT system” however, schools will need to be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”
It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

2. Aims

The school must ensure that it appropriately safeguards staff and students through an effective online filtering and monitoring regime.

3. Requirements of online Filtering and Monitoring

The school must ensure that internet systems are robust and appropriate for use by:

- Being able to demonstrate how its systems manage effective filtering and monitoring by the completion of an annual safety check, including filtering and monitoring (refer to Appendix A and B for supporting documentation).
- The completion of these checks will allow the school to construct a risk assessment that considers the risks that both students and staff may encounter online.

4. Roles and Responsibilities

The Governing Body

The Governing Body is responsible for monitoring the effectiveness of safeguarding within the school and making checks on the appropriateness of online filtering and monitoring systems.
The Governing Body will monitor the effectiveness of this policy and hold the headteacher to account for its implementation. They should be doing all that they reasonably can to limit students’ exposure to online risks through the school’s IT system, HARRAP.

Headteacher

The headteacher and appropriate senior leaders, are responsible for ensuring that this policy is adhered to, and that:

- The school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of students, and provide them with a safe environment in which to learn.
- They consider the age range of students, the number of students, how often they access the IT system.
- Leaders conduct a risk assessment as required by the Prevent Duty.

- The school keeps a breast of statutory changes of government policy, and that the school meets all legal requirements for online monitoring and filtering.
- The school implements the relevant statutory arrangements for online monitoring and filtering.

Other staff

Other staff will 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.
This policy will be monitored and reviewed on a three-year cycle or as required by legislature changes. This policy links to the following policies and procedures:

- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- E-safety Policy

4. Monitoring

- The school has daily access filtering alert which informs the Welfare Manager of any safeguarding concerns.
- Pupils have personal users, which filter access of all pupils across the school.
- The School ICT provider, HARRAP, sent monthly reports outlining any safeguarding concerns.
- The Welfare Manager, alongside the Headteacher, go through the monitoring checklist on a termly bases.
- All checks will be in line with the whole safeguarding and monitoring procedures.

Filtering and Monitoring Checklist Register

In line with the DfE filtering and monitoring standards in schools and colleges, this checklist template has been developed as a basis to support schools and colleges in meeting the required standards. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

Last updated:	Date:	Name/Position:

Roles and Responsibilities

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	
Senior Leadership Team Member	Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	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	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	

Reviewing your filtering and monitoring provision

Filtering System	
Filtering Provider and System	
Date Procured	
Date last reviewed	

Monitoring System	
Monitoring Provider and System	
Date Procured	
Date last reviewed	

Review Team [should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor]	
Review Date	
Previous Review Date	
Link to last review	

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

all staff know how to report and record concerns	
filtering and monitoring systems work on new devices and services before release to staff / pupils	
blocklists are reviewed and they can be modified in line with changes to safeguarding risks	

Recommendations / Mitigating Actions

Data Protection Impact Assessment

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

Link to DPIA	
Conducted by	
Date conducted	

Regular Reports

Type of Report	Filtering / Monitoring
Producer of report	
Recipient of report	
Frequency of report	

Monitoring data is received in a format that your staff can understand	
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	

System Checks

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Confirm 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)	

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result