Warwick Schools Foundation

Author	Rebecca Jessup/Jenny Parkinson Mills
Version	3.3
Date of Approval	
Review	October 2024
Next Approval	October 2025

Amendment	January 2025
	Change to include the new Filtering and Monitoring system at The Kingsley School DSL staff change for The Kingsley School

WEB FILTERING AND MONITORING POLICY

1.0 Introduction to Filtering

1.1 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 important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. The Foundation therefore has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in its schools.

1.2 The Foundation's filtering system (Smoothwall for Myton Road site, and for The Kinglsey School with effect from January 2025) will be operational, up to date and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

1.3 The Foundation's filtering system should:

- filter all internet feeds.
- 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.

2.0 Introduction to Monitoring

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

2.2 The Foundation's monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies will 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 (Senso monitoring software is available for use by staff in school computing suites)
- network monitoring using log files of internet traffic and web access (through Smoothwall)
- individual device monitoring through software (through Smoothwall)

2.3 Filtering and Monitoring Responsibilities

- DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include:

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Anne Wilson – Safeguarding Governor
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	Rebecca Jessup – Foundation Director of Safeguarding And Jenny Parkinson-Mills – Foundation Director of Digitally Enabled Learning

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	Richard Thomson – Senior Deputy Head Pastoral (WSS) Shirley Watson – Senior Deputy Head Pastoral (KHS) Deborah Ward – Head of Prep (WPS) Heather Mellor – Deputy Head (WJS) Martha Bruchez – Assist Head Teacher (TKS) Dawn Morgan – Pastoral (TKS)
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • Providing filtering and monitoring reports • completing actions following concerns or checks to systems	Jenny Parkinson-Mills – Foundation Director of Digitally Enabled Learning
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	

3.0 Policy Statements

3.1 Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the Foundation IT support team. Illegal content is filtered by the filtering provider (Smoothwall) by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the schools to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network (eg. BYOD devices and staff mobile phones), filtering and monitoring will be applied that is consistent with Foundation practice.

- There is a filtering and monitoring system (Smoothwall) in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
    - Daily reports of web activity will be sent to school DSLs
    - Live alerts relating to pupils will be received and actioned by the DSL of the appropriate school
    - Live alerts relating to staff will be received and actioned by the Foundation Director of Safeguarding
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader (eg. Foundation Director of Safeguarding, Foundation Director of Digitally Enabled Learning, school DSL) in the agreement of the change.
- Mobile devices that access the Foundation's internet connection (whether school or BYOD/personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The Foundation has provided enhanced/differentiated user-level filtering through the use of the Smoothwall system (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)
- The data collected on the monitoring system comprises only school username, URLs searched on site and harmful/dangerous key words/terms searched. This data is retained on Smoothwall for a period of 2 months. Learners are made aware of the data collected through their acceptable use policy.

4.0 Changes to Filtering and Monitoring Systems

4.1 There is a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

- Users may request changes to the filtering system by completing the “unblock website request form” or through an email to the IT support helpdesk (support@warwickschools.co.uk).
- The grounds on which changes may be permitted or denied will be shared with the user and logged by the Foundation IT support team.
- A senior responsible person will agree to the change before it is made (eg. Foundation Director of Digitally Enabled Learning / Foundation Director of Safeguarding / school DSL).
- An audit of changes to the filtering will be maintained by the Foundation IT support team.
- The reporting procedures for live alerts from the monitoring system will be reviewed by the Foundation Director of Safeguarding.
- DSLs and the Foundation Director of Safeguarding can request changes to the categories reported on in their weekly web activity reports to ensure the monitoring data is as helpful as possible when trying to protect their pupils and staff.
- DSLs and the Foundation Director of Safeguarding can request changes to the categories and key words used to prompt a live alert to ensure the monitoring is as effective as possible for the users that they are trying to protect.

5.0 Filtering and Monitoring Review and Checks

5.1 To understand and evaluate the changing needs and potential risks of the schools, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by the Foundation Director of Safeguarding and the Foundation Director of Digitally Enabled Learning. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

6.0 Reviewing the filtering and monitoring provision

6.1 A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

6.2 The review will take account of:

- the risk profile of learners, 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 learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)

- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

6.3 To make the filtering and monitoring provision effective, the review will 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

6.4 The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. introduction of BYOD
- new technology is introduced

7.0 Checking the filtering and monitoring systems

7.1 Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

7.2 When filtering and monitoring systems are checked this will include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on 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

7.3 Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

8.0 Training and Awareness

8.1 It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

8.2 Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

8.3 Those with specific responsibilities for filtering and monitoring (Safeguarding Governor, DSLs, Foundation Director of Safeguarding and Foundation Director of Digitally Enabled Learning) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

8.4 Learners are made aware of the expectations of them and the data collected:

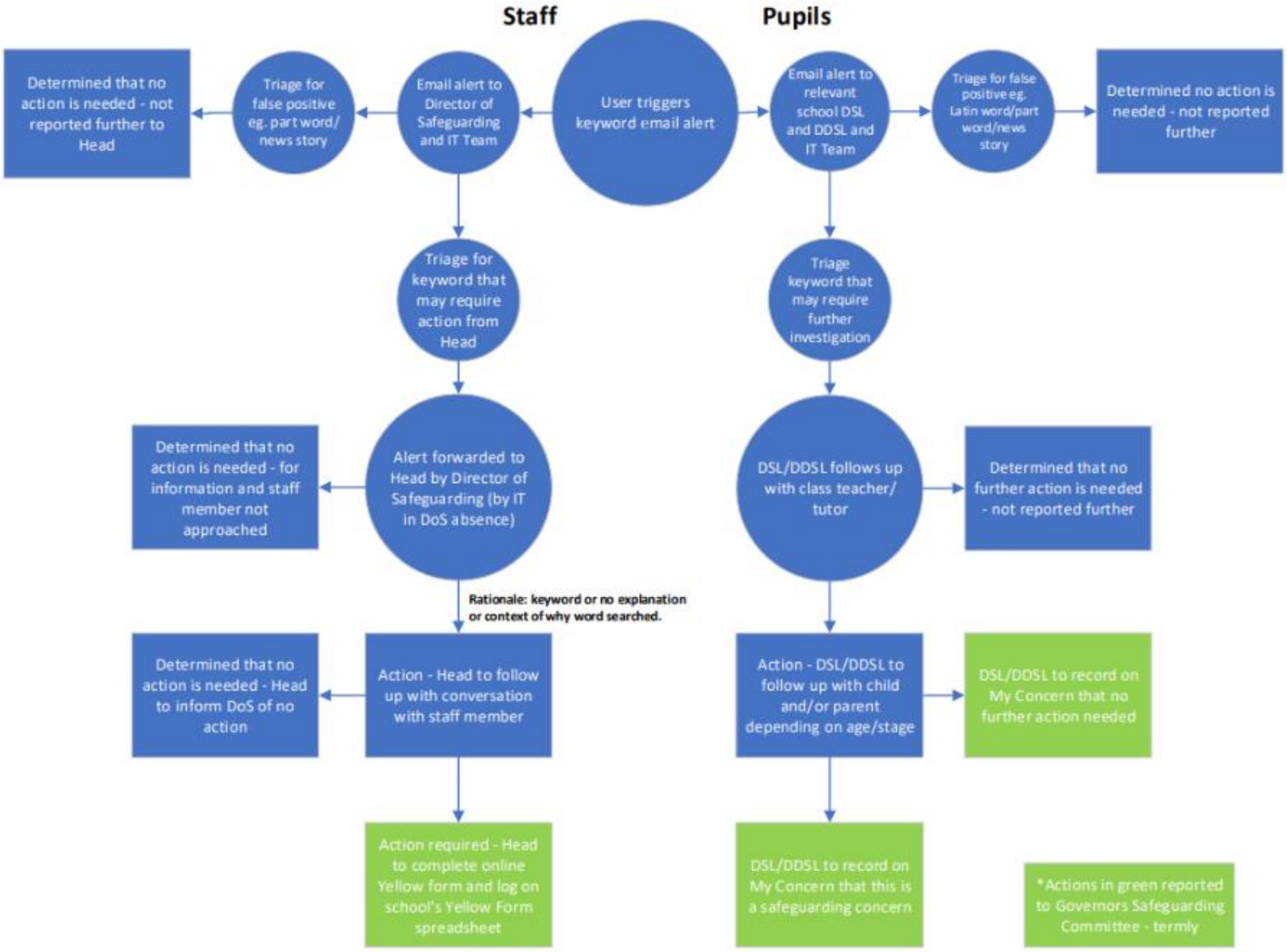
- in sessions at the start of the academic year, when they join the BYOD programme and as part of their PSHEE curricula
- through the pupil acceptable use agreements

8.5 Parents will be informed of the school's filtering policy through the pupil acceptable use agreements and through online safety awareness sessions.

9.0 Audit of Monitoring, Reporting and Review

9.1 Governors/Foundation Director of Safeguarding/DSL/Foundation Director of Digitally Enabled Learning will ensure that full records are kept of:

- Training provided
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems


Staff
Pupils
User triggers keyword email alert
Email alert to Director of Safeguarding and IT Team
Triage for false positive eg. part word/ news story
Determined that no action is needed - not reported further to Head
Triage for keyword that may require action from Head
Alert forwarded to Head by Director of Safeguarding (by IT in DoS absence)
Determined that no action is needed - for information and staff member not approached
Rationale: keyword or no explanation or context of why word searched.
Action - Head to follow up with conversation with staff member
Determined that no action is needed - Head to inform DoS of no action
Action required - Head to complete online Yellow form and log on school's Yellow Form spreadsheet
Email alert to relevant school DSL and DDSL and IT Team
Triage for false positive eg. Latin word/part word/news story
Determined no action is needed - not reported further
Triage keyword that may require further investigation
DSL/DDSL follows up with class teacher/ tutor
Determined that no further action is needed - not reported further
Action - DSL/DDSL to follow up with child and/or parent depending on age/stage
DSL/DDSL to record on My Concern that no further action needed
DSL/DDSL to record on My Concern that this is a safeguarding concern
*Actions in green reported to Governors Safeguarding Committee - termly