SPENCER
ACADEMIES TRUST

Filtering & Monitoring Policy

September 2026

Contents

Overview 2
Online Risks through the Four Domains: 4Cs 3
SAT Approach to Filtering and Monitoring 4
DSL Team Responsibilities and Expectations 5
IT Services Team Responsibilities and Expectations 6
Contacts 7
- Strategic Safeguarding and Filtering & Monitoring Contacts 7
- Filtering & Monitoring Supplier Contact 7

In Practice 7
- Preventative/Proactive 7
- Responsive/Reactive 7

Technology Overview 8
- Smoothwall Cloud Filter Overview 8
- Smoothwall Monitor Overview 8

Configuration Overview 9
- Smoothwall Configuration: Academies 9
- Out of School hours, including school holidays 9
- Smoothwall Configuration: Central Team 10

Appendices 11
- Appendix 1: Alert Procedure for Students 11

Overview

This policy applies to all children and staff of Spencer Academies Trust and is designed to support effective safeguarding when using Trust-owned devices. It sets out the responsibilities, expectations and controls that help ensure technology is used safely, securely and appropriately, protecting the welfare of children and staff both on and off Trust premises.

The Trust has developed comprehensive policies, procedures, guidance and training to ensure that we are well prepared to safeguard children and staff while they are using the IT equipment and digital services provided across our Trust. In developing this approach, we have considered the Department for Education's (DfE) Filtering and Monitoring Standards and ensured alignment with the latest version of Keeping Children Safe in Education (KCSIE).

Alongside our policies and procedures, the Trust delivers a comprehensive Personal Development and Online Safety curriculum that promotes responsible, safe and informed use of technology. This proactive educational approach complements our filtering and monitoring arrangements, enabling us to educate children and staff, identify potential safeguarding concerns, and respond appropriately when risks arise.

This document outlines the Trust's expectations, responsibilities and operational requirements in relation to filtering and monitoring. It provides academy leaders and staff with a clear framework for ensuring compliance with safeguarding requirements and maintaining a safe digital environment for all children and staff.

Online Risks through the Four Domains: 4Cs

KCSIE refers to the **4 Cs** that must be considered and appropriately planned for when filtering and monitoring student and staff activities online:

Content: What children see online - being exposed to illegal, inappropriate, or harmful content, for example: violence, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. This also includes AI – generative content which exposes children to misinformation and harmful material.

Contact: **Who children interact with online -** being subjected to harmful online interaction with other users; for example: peer to peer pressure, adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. This also includes harmful interactions with AI-Chatbots or online users.

Conduct: How children behave online - online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying. This also includes the creation or sharing of AI-generated intimate images, deepfakes or other abusive material.

Commerce: Commercial risks - such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

SAT Approach to Filtering and Monitoring

Spencer Academies Trust operates a comprehensive filtering and monitoring framework designed to safeguard children and staff while using Trust-managed devices, networks and digital services. Our approach combines technology, processes, training and oversight to support a safe digital environment across all academies.

Filtering controls are implemented across the Trust to protect children and staff from harmful, inappropriate and illegal content, whilst supporting teaching, learning and business operations. Our monitoring arrangements help identify potential safeguarding concerns, indicators of risk and inappropriate use of technology, enabling timely intervention and support where required.

The Trust's filtering and monitoring platform is provided by Smoothwall, which delivers web filtering, device monitoring and safeguarding alerting capabilities across our managed environment. These systems help protect children and staff from harmful, inappropriate and illegal content, whilst providing visibility of potential safeguarding concerns and emerging risks.

Monitoring capabilities are deployed across Trust-managed devices to support the identification of safeguarding concerns and enable timely intervention where required. Where users access Trust services through Bring Your Own Device (BYOD) or guest wireless networks, web filtering controls remain in place; however, device-level monitoring is not available as these devices are not managed by the Trust. All users remain subject to the Trust's safeguarding policies, acceptable use expectations and procedures when accessing Trust systems and services.

Designated Safeguarding Leads (DSLs) receive appropriate training to access, review, analyse and respond to information generated by the Trust's filtering and monitoring systems. Awareness and understanding of the Trust's filtering and monitoring arrangements extends across academy leadership teams, the Executive Leadership Team and the Board of Directors, ensuring appropriate governance, accountability and oversight.

In line with the Department for Education's Filtering and Monitoring Standards and the latest version of Keeping Children Safe in Education (KCSIE) the Trust has:

- Clearly identified and assigned roles and responsibilities for the management, review and oversight of filtering and monitoring systems.
- Established processes for the regular review and evaluation of filtering and monitoring arrangements.
- Implemented monitoring strategies that support the safeguarding and wellbeing of children and staff.
- Applied proportionate filtering controls that block harmful and inappropriate content whilst avoiding unnecessary restrictions on teaching, learning and legitimate educational activities.
- Ensured that safeguarding concerns identified through monitoring processes are reviewed and acted upon in accordance with Trust safeguarding procedures.

Through this combined approach of technology, governance, professional judgement and safeguarding oversight, Spencer Academies Trust seeks to maintain a safe, secure and supportive digital environment for all children and staff.

DSL Team Responsibilities and Expectations

The DSL teams at our individual academies and central team are responsible for regularly monitoring, reviewing, responding to, and reporting on internet filtering and monitoring. While it is recognised that different team structures will mean there is variation on how the responsibilities and expectations are executed, the following actions must be completed by the agreed deadlines:

- Ensuring that live monitoring of children and staff devices is enabled across the academy, including devices that have been provided by the academy to children for remote learning purposes.
- Immediate review of any alerts received through Smoothwall Monitor. Standard safeguarding procedures should then be followed. The alerts triaged by Smoothwall at Level 3 and above will automatically be documented on CPOMS. As a minimum standard, all members of the DSL team will receive an additional email alert.
- A weekly review of filtering reports will take place. This will identify blocked websites, most watched/viewed websites and videos, and any emerging trends. Each academy will take a proactive approach to reviewing and utilising the information to educate children and staff, as well as providing interventions and support for those who need it.
- A weekly review of monitoring reports will take place. This will identify an overview of monitoring alerts that have been generated. Each academy will take a reactive approach to reviewing and utilising the information to educate children and staff, as well as providing support for those who need it.
- The SLT member responsible for filtering and monitoring should carry out at least an annual review of filtering and monitoring arrangements. This should be carried out with the support of the DSL and IT Services. The review should consider whether the arrangements effectively address the 4Cs (Content, Contact, Conduct and Commerce).
- Termly DSL Network meetings take place with opportunity to discuss updates, analysis and trends. DSL can also feedback to the Head of Safeguarding who will subsequently coordinate with the Director of Strategic ICT & Infrastructure any changes to be made to the configuration considering feedback from meetings.
- In addition to the above, the Director of Inclusion will provide termly updates, giving an overview of all our Trust data via the Smoothwall report to Board of Directors through the Safeguarding & Inclusion committee.

IT Services Team Responsibilities and Expectations

The IT Services Team works in partnership with the Education & Inclusion Team to develop, maintain and continuously improve the Trust's filtering and monitoring arrangements. Together, they ensure that technical safeguarding controls are effective, proportionate and aligned with statutory safeguarding requirements, protecting children and staff from online harms whilst supporting teaching, learning and business operations.

The Trust's filtering and monitoring solutions are configured to prevent access to harmful, inappropriate and illegal content, whilst avoiding unnecessary restrictions on legitimate educational activity and school administration. Through ongoing collaboration with safeguarding leaders, the IT Services Team ensures that filtering and monitoring controls remain responsive to emerging risks, changing technologies and evolving safeguarding requirements.

The ongoing responsibilities of the IT Services Team include:

- Providing technical expertise and support to academies in relation to filtering, monitoring and safeguarding technologies.
- Maintaining comprehensive audit records of configuration changes and system administration activities through regular review and reporting processes.
- Managing and configuring filtering and monitoring schedules, including holiday and out-of-hours arrangements, in collaboration with individual academies.
- Supporting the continuous development of Designated Safeguarding Leads (DSLs) and other authorised users through training, guidance and technical briefings on filtering and monitoring systems.
- Reviewing emerging threats, safeguarding trends and product developments to ensure Trust systems remain effective and aligned to best practice.
- Communicating significant changes, enhancements or service impacts relating to filtering and monitoring systems to relevant stakeholders.
- Working alongside safeguarding leaders to ensure filtering and monitoring arrangements remain effective, proportionate and compliant with the Department for Education's Filtering and Monitoring Standards and the latest version of Keeping Children Safe in Education (KCSIE).

Contacts

Strategic Safeguarding and Filtering & Monitoring Contacts

Contact	Role	Telephone	Email
Sarah McAneny-Vincent	Executive Director of Inclusion	07855 175011	Smcaneny@spencertrust.org.uk
Fiona Hallam	Head of Safeguarding	07834 857338	Fhallam@spencertrust.org.uk
Matthew Taylor	Director of Strategic ICT & Infrastructure	07811 790155	MTaylor@spencertrust.org.uk
Alison Smith	Director of HR	07966 881311	Asmith@spencertrust.org.uk

Filtering & Monitoring Supplier Contact

Contact	Role	Email
John Meki	Smoothwall Account Manager	john.meki@smoothwall.com

In Practice

There are two essential approaches to safeguarding that we must ensure we have the correct policies and procedures in place to appropriately plan for. We always aim to be working proactively, preventing any concerns from arising through careful consideration and development of our offer. We know that this isn't always possible, and through the very nature of online technologies, there will always be a need to be reactive, ensuring we are suitably prepared to respond to an emerging need.

Below are two lists: one indicates our preventative measures, and the other outlines our responsive processes.

Preventative/Proactive

- Online Safety Policy
- Spencer Academies Trust Safeguarding and Child Protection Policies and Procedures
- Acceptable and Responsible Use Policy
- Web Filter reports
- Weekly monitoring procedures and reports
- Termly review and report to Governors and Board
- CPD designed to support in understanding and developing the use of filtering and monitoring data
- Online Safety Curriculum
- Curated list of applications that are deemed safe
- Mobile Device Management software

Responsive/Reactive

- Monitoring System alert
- Weekly monitoring
- Continued curation of a blocked keyword/website list based on contextual information
- Education and support for children based on individual identified needs from monitoring
- Code of Conduct

Technology Overview

Smoothwall Cloud Filter Overview

Smoothwall Cloud Filter is unlike any other filter in education. It assesses the permissibility of a web page, not by referencing published blocklists, as with some Filters, but by evaluating its content, context and construction at the point of request. This means harmful content is blocked the second it goes live. The hours, days, weeks and sometimes months required by other filters to recognise and block inappropriate content, (time in which children may see it) is a non-issue with Smoothwall. Students are protected in 100% real-time, all the time. No matter the content, no matter when it went live. Cloud Filter also comes with deep granular controls enabling us to determine who sees what, where and when enabling safe, age-appropriate online experiences for every student.

Smoothwall Monitor Overview

Smoothwall Monitor is an at-risk student and staff identification solution that monitors and analyses online activity for signs of self-harm, violence, grooming, inappropriate behaviour and bullying. By enabling early intervention, Smoothwall Monitor empowers schools and the wider organisation to take a proactive approach to student and staff safety.

AI technology identifies concerning online indicators or content and alerts designated staff. Alerts include the relevant context, including recent activity before and after the alert. This allows relevant staff to understand the context and react appropriately. Where necessary, AI identified alerts are passed to a human review team for moderation and then alerted to designated staff. For the most concerning alert content human reviewers contact designated staff by telephone.

Configuration Overview

Smoothwall Configuration: Academies

From 8am through to 5pm, the DSL team in each academy will be responsible for receiving and responding to any student alerts. There will be no less than 2 staff members receiving the alerts to avoid a single point of failure. Alerts for members of academy staff will be raised with the principal and other identified senior leader responsible for staff safeguarding.

Alerts for all academies (staff and students) will also be monitored by the Director of Inclusion and Head of Safeguarding. Alerts will be communicated via email, with the school telephone number and DSLs mobile numbers (where appropriate) on the software system for the Smoothwall Monitor team to use where necessary.

DSLs will be responsible for ensuring that there is an appropriate response to the Smoothwall alert. This may include assigning it to a particular staff member reviewing and investigating the alert and taking necessary steps in accordance with the Safeguarding and/or Behaviour Policy. When closing the alert upon a satisfactory conclusion, there should be a clear audit trail of the actions and decision making which has been part of the response. Alerts above a level 3 will be automatically integrated into CPOMS and should be actioned and recorded appropriately in line with Trust expectations.

Principals will respond to staff alerts by reviewing, investigating and taking necessary steps in line with the Safeguarding and/or Code of Conduct and will close the alert upon a satisfactory conclusion. Where deemed necessary this will be logged as a Low Level Concern on Every as per Trust expectations and procedures.

Misconduct or gross misconduct identified through our filtering and monitoring systems will be managed in line with trust procedures and the Disciplinary Policy will be followed accordingly.

Where filtering and monitoring identifies a welfare concern for a colleague, we will support through our wellbeing offer and the colleague will be provided with support for their health and wellbeing accordingly.

Where the concern relates to the Principal, the Director of Inclusion and Director of HR will be alerted.

Out of School hours, including school holidays

Out of school hours alerts will be directed to the Director of Inclusion and Head of Safeguarding as well as any designated staff in individual academies who have requested access to alerts out of school hours. There will be no less than 2 staff members receiving the alerts to avoid a single point of failure. Alerts will be communicated via email, with the relevant contact numbers stored on the software system for the Smoothwall Monitor team to use where necessary.

Where necessary, individual designated academy staff may be contacted for further information or to discuss next steps.

Smoothwall Configuration: Central Team

The Director of Inclusion and Director of Human Resources will be responsible for receiving and responding to any central team alerts. There will be no less than 2 staff members receiving the alerts to avoid a single point of failure.

Alerts will be communicated via email, with the relevant contact details stored on the software system for the Smoothwall Monitor team to use where necessary.

The Director of Inclusion and/or Director of HR will liaise, as appropriate, with the line manager of the member of staff who will review and investigate the alert and take necessary steps in accordance with the Safeguarding, Code of Conduct or Disciplinary Policy. Where deemed necessary this will be logged as a Low Level Concern on Every as per our expectations and procedures.

Misconduct or gross misconduct identified through our filtering and monitoring systems will be managed in line with trust procedures and the Disciplinary Policy will be followed accordingly.

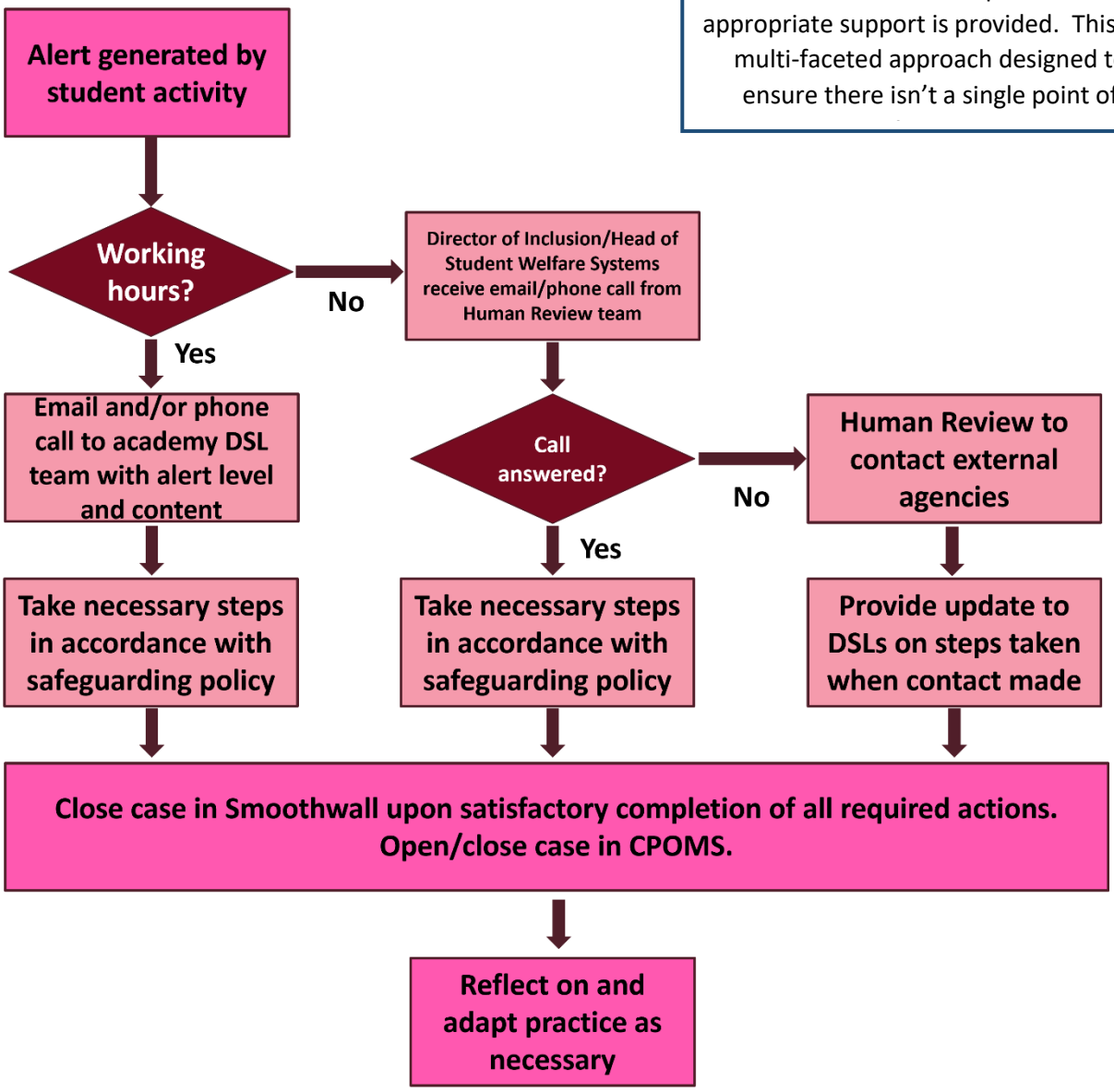
Where filtering and monitoring identifies a welfare concern for a colleague, we will support through our wellbeing offer and the colleague will be provided with support for their health and wellbeing accordingly.

Where the concern relates to an Executive Leader the CEO will be alerted. Where the concern relates to the CEO the Chair of the Board will be alerted.

Appendices

Appendix 1: Alert Procedure for Students

In the event that an alert is generated by Smoothwall through a students use of a device, following the steps below will ensure the child is kept safe and appropriate support is provided. This is a multi-faceted approach designed to ensure there isn't a single point of



Approved by: S McAneny-Vincent	**Date:** 1st September 2026
Last Reviewed On: 4th August 2026	
Next Review Due By: September 2027	

Version History

Version History	Approved By	Revision Date	Description of Change	Author
2	SMV	01/09/2025	Updated KCSIE referenced dates Updated 4 Cs in line with new definitions in KCSIE 2025	SMV
3	SMV	04/08/2025	Updates KCSIE references Added information into the 4Cs Additional information around AI content Additional information about DSL and SLT responsibilities	MT FH