SPENCER
ACADEMIES TRUST

Filtering & Monitoring Policy

September 2025

Contents

1. Overview 2
2. SAT Approach to Filtering & Monitoring 2
3. DSL Team Responsibilities & Expectations 4
4. IT Team Responsibilities & Expectations 5
5. Important Contacts 5
6. In Practice 6
7. Smoothwall Cloud Filter Overview 7
8. Smoothwall Monitor Overview 8
9. Smoothwall Configuration: Academies 8
10. Smoothwall Configuration: Central Team 9
Appendix 1: Alert Procedure for Students 11

Overview

This policy applies to all employees of Spencer Academies Trust and aims to ensure effective safeguarding when children are using the internet is at the heart of all decision-making.

We have developed our policies and procedures and delivered guidance and training to ensure that we are prepared to safeguard our children while they are using the IT equipment we provide in our academies. In order to provide this guidance, we have consulted DfE standards for filtering and monitoring and ensured compliance with Keeping Children Safe in Education (KCSiE, 2025).

Alongside our policy, practice and procedures we have a comprehensive Personal Development and online safety curriculum promoting a proactive approach that sits alongside our reactive monitoring and filtering process.

Contained within this document are the expectations and responsibilities for our academies around effective filtering and monitoring.

SAT Approach to Filtering and Monitoring

KCSiE (2025) refers to the **4 C's** that must be considered and appropriately planned for when filtering and monitoring student and staff activities online:

> **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
>
> **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
>
> **conduct:** 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.

commerce: 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/).

We have a comprehensive setup for network security and monitoring. Our system includes robust monitoring and alerting functionalities that are deployed across all registered devices accessing our networks, ensuring the safety and well-being of staff and students by tracking and alerting on any concerning activity. Additionally, we employ advanced filtering protection to safeguard the network from various threats and control access to potentially harmful content.

This combination provides strong control over monitoring online behaviour and protecting the network from malicious activities.

Our current filtering and monitoring provider is Smoothwall.

Our DSLs are trained in accessing, utilising, analysing and reporting from the software. Leadership at all levels, including the Board, Executive Leadership Team and academy teams also have an awareness and understanding of the software in place.

As prescribed in the DfE Filtering & Monitoring Standards we have ensured that we have:

- Identified and assigned roles and responsibilities to manage filtering and monitoring systems.
- Ensured the review of our filtering and monitoring provision monthly.
- Developed effective monitoring strategies to meet the safeguarding needs of students and staff.
- Blocked harmful and inappropriate content without unreasonably impacting teaching and learning, taking into consideration that 'over blocking' can lead to unreasonable restrictions as to what children can be taught with regard to online teaching and learning.

In addition to our filtering solution with Fortinet, we also have individual device monitoring through Smoothwall Monitor.

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 student and staff devices is enabled across the Trust, 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. Expectations are set for response and follow-up times. The alert should be documented on CPOMS. As a minimum standard, all members of the DSL team will receive the 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 students, as well as providing interventions and support for those who need it.
- Weekly reports will be produced to provide an overview to key stakeholders of the activity on the devices. These reports will detail the findings and actions identified.
- Half-termly Regional Hub and DSL Network meetings between DSLs across the Trust to discuss updates, analysis and trends. The Head of Student Welfare Systems will subsequently coordinate with the Director of Strategic ICT & Infrastructure any changes to be made to the configuration in light of 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. This will include sharing the number of alerts, how many led to action being taken, the number of blocked searches and term-on-term comparisons.

IT Team Responsibilities and Expectations

The IT team have worked alongside the education team to configure our filtering and monitoring solutions so that the solution blocks internet access to harmful sites and inappropriate content without unreasonably impact on teaching and learning or school administration. The ongoing responsibilities of the IT team include:

- Providing technology support to respond to any emerging needs that the academy is unable to complete themselves.
- Running monthly audit logs to maintain a record of changes made on an individual and trust-wide basis.
- Configuring Monitoring and filtering for holiday timings in collaboration with each academy.
- Providing periodic CPD to DSLs and other monitoring and filtering users to inform them of new updates and emerging trends that require additional understanding of the technical elements of monitoring or filtering products.
- Keeping schools informed of new developments within monitoring and filtering solutions, or potential disruption as a result of software updates or changes to setup.

Important Contacts

IT Services Helpdesk

Email: ITSHelpdesk@spencertrust.org.uk

Web: itshelpdesk.spencertrust.org.uk

Sarah McAneny-Vincent – Director of Inclusion

07855175011

Smcaneny@spencertrust.org.uk

Fiona Hallam – Head of Student Welfare Systems

07834 857 338

Fhallam@spencerturst.org.uk

Matt Taylor – Director of Strategic ICT & Infrastructure

0781 179 0155

MTaylor@Spencertrust.org.uk

Alison Smith – Director of HR

07966881311

Asmith@spencertrust.org.uk

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

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.

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 Student Welfare Systems. 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 Student Welfare Systems 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.

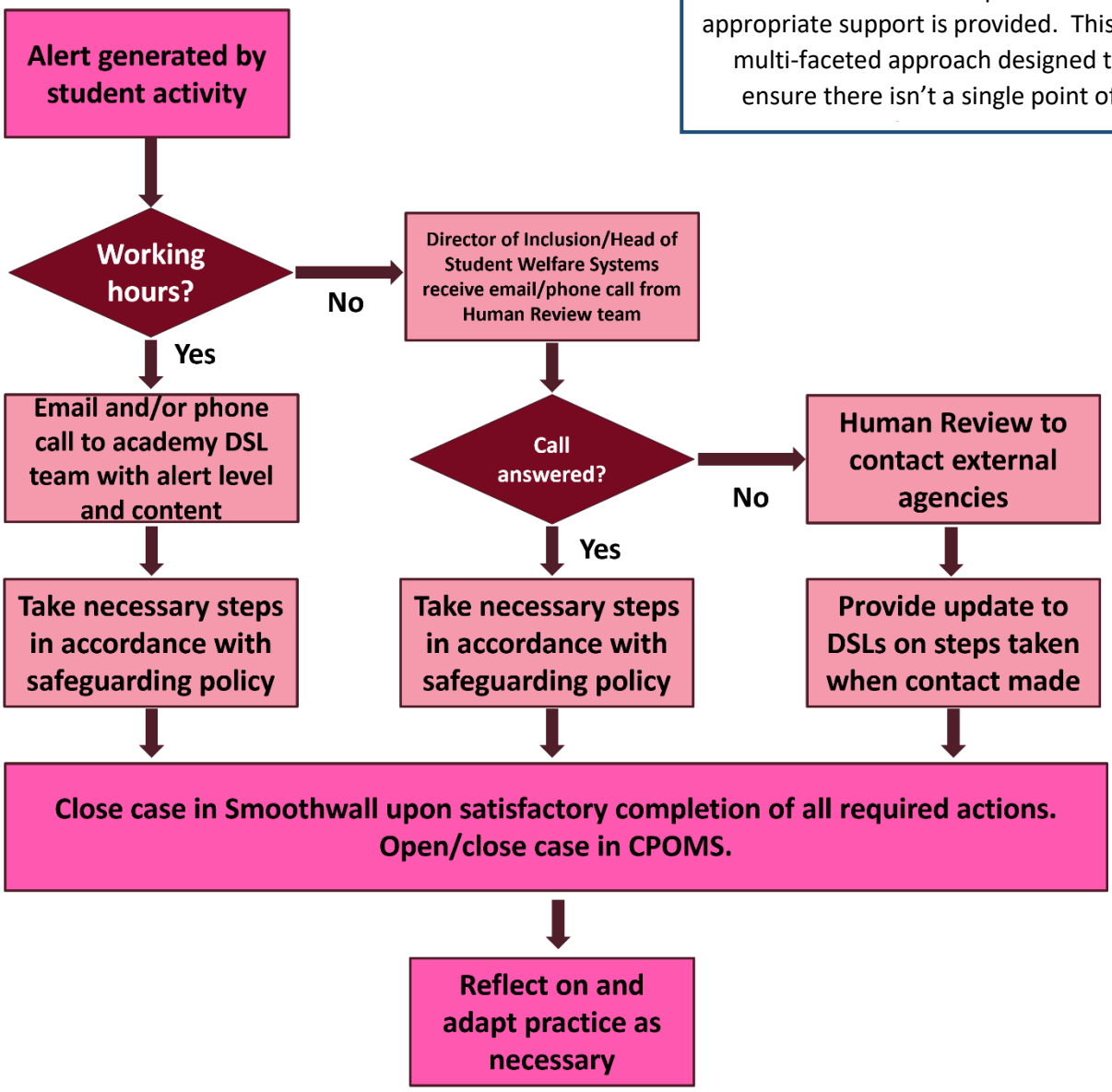
Misconduct or gross misconduct identified through our filtering and monitoring systems will be managed in line with trust procedures and the Disciplinary Policy will be followed accordingly.

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.

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 2025
Last Reviewed On: 1st September 2025	
Next Review Due By: September 2026	

Version History

Version History	Approved By	Revision Date	Description of Change	Author
2	SMV	1/9/25	Updated KCSIE referenced dates Updated 4 Cs in line with new definitions in KCSIE 2025	SMV