Filtering and Monitoring Policy

Key Document Details:			
Author:	Trust IT Manager	**Department:**	Central Services
Reviewer:	Headteachers	**Version No:**	1.0
Last Review:	August 2023	**Next Review:**	August 2026
Approver:	Executive Team	**Date Ratified:**	

Contents

Document Change History

Date:	Version:	Description of Changes:
August '23	1.0	New policy

Mission Statement

"To nurture and develop all people in our Trust so that they reach their full potential academically, vocationally, and personally, including being positive role models for future generations in the community. We will achieve this by providing high quality values-based education that cultivates employability and life skills making our schools the first choice for young people, parents, carers, staff and employers."

Values

The values of Respect, Excellence, Collaboration, Independence, Perseverance, Enjoyment, Leadership, Integrity and Care are central to everything we do at the Skills for Life Trust.

Statement of Equality

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Purpose

Each academy within the trust will have its own unique demands and use of the internet. However, all academies must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime. Registered childcare providers 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, 2015).

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 also become a significant component of many safeguarding issues, such as child sexual exploitation, radicalisation and sexual predation. Technology often provides the platform that facilitates harm.

An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes 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."

Requirements

All academies within the Trust must ensure that internet systems are robust and appropriate for use. Academies are required to follow the Trust guidance below.

Guidance

Skills for Life Trust require all schools to be able to demonstrate how their systems manage effective filtering and monitoring by the completion of an annual safety check, including filtering and monitoring. The Trust will provide an audit template (appendix 1) for use in schools.

The completion of these checks will allow all leaders to construct a risk assessment

Actions To Take by the School	Actions to take by the Trust
Complete the annual filtering and monitoring standards audit (Appendix 1)	Check that the school has completed annual Online Safety Checks (Filtering and Monitoring)
Complete a risk assessment that considers the outcomes of checks and limits the risks that children and staff may encounter online	Check to see a risk assessment summary for children and staff is in place that satisfies the Prevent Duty

Roles and Responsibilities

The Board of Trustees has delegated the responsibility for monitoring the way in which online monitoring and filtering is implemented within each academy to the Senior Leadership Team (SLT) of each Academy within the Trust.

The SLT are responsible for monitoring the effectiveness of safeguarding within schools and making checks on the appropriateness of online filtering and monitoring systems in academies.

The Board of Trustees/CEO

The board of trustees/CEO will monitor the effectiveness of this policy and hold the headteacher/principal to account for its implementation. They should be doing all that they reasonably can to limit children's exposure to risks online risks through the school's IT system.

Headteacher

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

- Their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn.
- They consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.
- Leaders conduct an annual filtering and monitoring standards audit (Appendix 1) and return the completed document to the Trust IT Manager
- The school keeps abreast 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.

Academy staff

Academy 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.

Links with other policies

This policy will be monitored as part of the Trust's annual internal review 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 Policy
- Child Protection and Safeguarding Policy

Appendix 1

Filtering and monitoring standards audit

Name of school	
Date audit completed	
Audit completed by	

Overview

[This section should be completed once the rest of the audit has been conducted. Boards should record whether the school meets each area of the filtering and monitoring standards.]

Area of the standards	Status (fully met / partially met / not met)	Notes
Identifying and assigning roles and responsibilities to manage filtering and monitoring systems		
Reviewing filtering and monitoring provision		
Blocking harmful and inappropriate content, without unreasonably impacting teaching and learning		
Monitoring strategies that meet the school's safeguarding needs		

Identifying and assigning roles and responsibilities to manage filtering and monitoring systems

Criteria	Status (fully met / partially met / not met)	Further action to meet the criteria	Additional notes
A member of the SLT and a governor have been assigned responsibility for ensuring the filtering and monitoring standards are met.			
The roles and responsibilities of staff have been identified and assigned.			
The roles and responsibilities of third parties, e.g. external service providers, have been identified and assigned.			
The SLT understands it is responsible for: • Procuring filtering and monitoring systems. • Documenting decisions on what is blocked or allowed and why. • Reviewing the effectiveness of the school's provision. • Overseeing reports. • Making sure that all staff understand their role, are			

appropriately trained, are following policies, processes and procedures, and act on reports and concerns.			
The DSL takes a lead responsibility for safeguarding and online safety, including overseeing and acting on: • Filtering and monitoring reports. • Safeguarding concerns. • Checks to filtering and monitoring systems.			
The ICT service provider has technical responsibility for: • Maintaining filtering and monitoring systems. • Providing filtering and monitoring reports. • Completing actions following concerns or checks to systems.			
The ICT service provider works with the SLT and DSL to:			

• Procure systems. • Identify risk. • Carry out reviews. • Carry out checks.			
Senior leaders work closely with governors, the DSL and ICT service providers in all aspects of filtering and monitoring.			
The DSL works closely with ICT service providers to meet the needs of the school.			
Overall status of this standard (fully met/partially met/not met)			
Further action needed to meet the standard			
Additional notes			

Reviewing filtering and monitoring systems

Criteria	Status (fully met / partially met / not met)	Further action to meet the criteria	Additional notes
Overall review			
Procedures are in place to ensure filtering and monitoring provision is reviewed at least annually, or when: • A safeguarding risk is identified. • There is a change in working practice. • New technology is introduced.			
The review is conducted by members of the SLT, the DSL and the ICT service provider, and also involves the governor responsible for filtering and monitoring.			
The review is used to understand: • The risk profile of pupils – factors to consider include age, SEND and EAL. • What the school's filtering system currently blocks or allows and why. • Any outside safeguarding influences, e.g. county lines.			

• Any relevant safeguarding reports. • The digital resilience of pupils. • Teaching requirements, e.g. RSHE and PSHE. • The specific use of the school's chosen technologies, including arrangements for bringing devices from home. • What related safeguarding and technology policies the school has in place. • What checks are currently taking place and how resulting actions are handled.			
The review is used to inform: • Related safeguarding or technology policies and procedures. • Roles and responsibilities. • Staff training. • Curriculum and learning opportunities. • Procurement decisions.			

• What is checked and how often. • Monitoring strategies.			
The result of the review is recorded and made available to those entitled to inspect the information.			
Checks			
Procedures for additional checks of filtering and monitoring provision are in place.			
When checking filtering and monitoring systems, the school makes sure the system set up has not been changed or deactivated.			
The checks include a range of: • School-owned devices and services, including those used off site. • Geographical areas across the site. • User groups, e.g. staff, pupils and visitors.			
A log of checks is maintained which records:			

• When the checks took place. • Who did the check. • What was tested or checked. • Resulting actions.			
The school makes sure that: • All staff know how to report and record concerns. • Filtering and monitoring systems work on new devices and services before releasing them to staff and pupils. • Blocklists are reviewed and they can be modified in line with changes to safeguarding risks.			
Overall status of this standard (fully met/partially met/not met)			
Further action needed to meet the standard			

Additional notes	

Blocking harmful and inappropriate content, without unreasonably impacting teaching and learning

Criteria	Status (fully met / partially met / not met)	Further action to meet the criteria	Additional notes
The governing board supports the SLT to procure and set up systems which meet the filtering and monitoring standards and the risk profile of the school.			
The school's filtering provider is: • A member of the 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).			
[Schools that procure filtering provision with a broadband service] The filtering provision meets the needs of the school.			
The school's filtering system is operational, up-to-date and applied to all: • Users, including guest accounts. • School-owned devices.			

• Devices using the school broadband connection.			
The school's filtering system: • Filters all internet feeds, including any backup connections. • Is age- and ability-appropriate for the users, and is suitable for educational settings. • Handles multilingual web content, images, common misspellings and abbreviations. • Identifies technologies and techniques that allow users to get around the filtering, such as VPNs and proxy services, and blocks them. • Provides alerts when any web content has been blocked.			
Confirmation has been sought as to whether the filtering and monitoring provider can provide filtering on mobile or app technologies.			
A technical monitoring system is applied to devices using mobile or app content.			

The school's filtering system allows the identification of people who might be trying to access unsuitable or illegal content. The system allows the school to identify: • The device name or ID, IP address, and where possible, the individual. • The time and date of the attempted access. • The search term of content being blocked.			
Data protection impact assessments (DPIAs) are conducted where necessary.			
Staff are aware of reporting mechanisms and make a 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.			
The school meets the broadband and internet standards.			
The school meets the cyber security standards.			
Overall status of this standard (fully met/partially met/not met)			
Further action needed to meet the standard			
Additional notes			

Monitoring strategies that meet the school's safeguarding needs

Criteria	Status (fully met / partially met / not met)	Further action to meet the criteria	Additional notes
The monitoring strategy is informed by the filtering and monitoring review.			
The governing board supports the SLT to make sure effective device monitoring is in place which meets the standards and the risk profile of the school.			
Procedures are in place and made clear to staff regarding how to deal with any incidents.			
Device monitoring is managed by ICT staff or third-party providers, who: • Make sure monitoring systems are working as expected. • Provide reporting on pupil device activity. • Receive safeguarding training including online safety. • Record and report safeguarding concerns to the DSL.			

The school makes sure that: • Monitoring data is received in a format that staff can understand. • Users are identifiable to the school, so concerns can be traced back to an individual, including guest accounts.			
Technical monitoring systems are applied to mobile and app technologies.			
The monitoring provision identifies and alerts the school to behaviour associated with the following areas of risk outlined in 'Keeping children safe in education': • Content • Contact • Conduct • Commerce			
All members of staff: • Provide effective supervision. • Take steps to maintain awareness of how devices are being used by pupils.			

• Report any safeguarding concerns to the DSL.			
Monitoring procedures are reflected in the following policies and procedures: • Child Protection and Safeguarding Policy • Online Safety Policy • Acceptable Use Agreements • Privacy notices			
Data protection impact assessments (DPIAs) are conducted where necessary.			
The privacy notices of third parties are reviewed.			
The school meets the cyber security standards.			
Overall status of this standard (fully met/partially met/not met)			
Further action needed to meet the standard			

Additional notes	