HET Filtering and Monitoring Policy

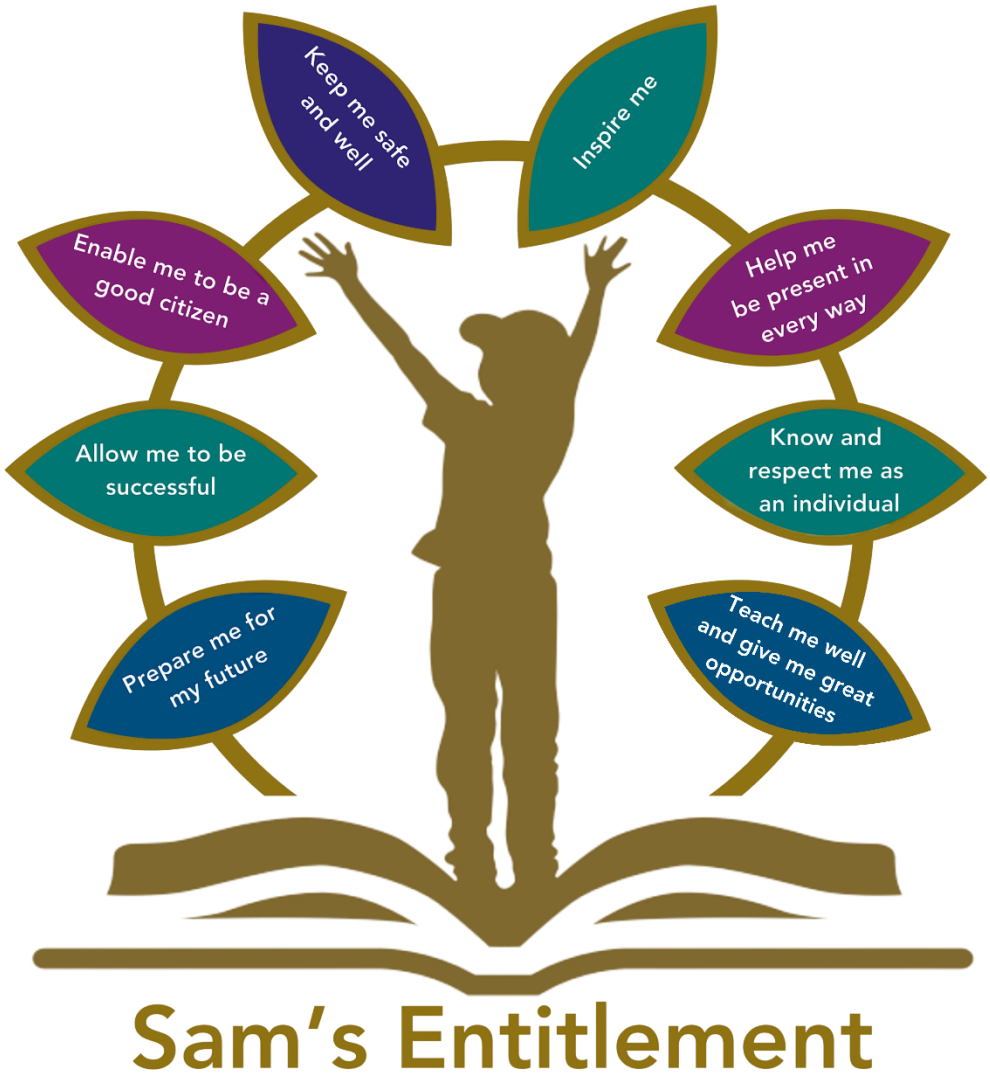
Reviewed on	November 26	Review frequency	Annual
Next review due	November 27	Template Yes / No	
Owner	Head of Safeguarding & Compliance	Approved by	DoPS

History of Policy Changes

Date	Page	Change	Origin of Change
Nov '26	5-6	Clarified expectations for reviewing, managing and recording Smoothwall monitoring alerts, including actions required for Level 1-5 alerts.	Operational clarification
	7-8	Updated guidance on recording monitoring alerts, including when alerts must be recorded on CPOMS/MyConcern and when they can be managed within Smoothwall.	Operational clarification
	9-10	Strengthened School Leader responsibilities to include retaining evidence of annual filtering and monitoring reviews and resulting actions. Clarified governance arrangements by requiring a named SLT lead for filtering and monitoring.	Policy review
	11	Clarified expectations regarding evidence of annual reviews for assurance and inspection purposes.	Policy review
	Various	Minor amendments throughout to improve clarity and support consistent use of the Smoothwall monitoring platform.	Policy review

1. Introduction 3
2. Background and Aims of the policy 4
3. Definitions 5
4. Child-on-Child Abuse 6
5. HET Filtering & Monitoring expectations 6
6. Filtering system (Smoothwall) 7
7. New Online Monitoring system for September 2026 (through Smoothwall) 8
8. Reports 8
9. Recording pupil filtering and monitoring alerts 9
10. Devices loaned to pupils 10
11. Staff concerns (filtering only) 10
12. Responsibilities 10
13. Assurance and Inspection Readiness 12
14. Reviewing your provision 13
15. Support from HET MS staff 14
16. HET Safeguarding Reviews 15

17. Link to other HET Policies 15
18. Useful information and links 15



1. Introduction

"Hamwic Education Trust (HET) believe that all pupils should receive a high quality, enriching, learning experience in a safe and inclusive environment, which promotes excellence through a broad curriculum that prepares them for their future and opens doors to a diverse array of opportunities as well as that all pupils and adults within HET flourish as individuals and together."

This policy sets out HET's approach to filtering and monitoring in line with the requirements of Keeping Children Safe in Education (KCSIE), ensuring

appropriate systems are in place to safeguard pupils and staff from online risks.

2. Background and Aims of the policy

Filtering and monitoring are safeguarding tools designed to identify, prevent and respond to online risks, including child-on-child abuse, bullying, sexual harassment, harmful sexual behaviour, exploitation, radicalisation, self-harm, suicide ideation and risks posed by emerging technologies such as artificial intelligence.

All HET schools must ensure they safeguard their pupils and staff through an effective online filtering and monitoring regime; this should protect against potentially harmful and inappropriate online material.

Effective filtering and monitoring should be viewed as one element of a school's wider safeguarding arrangements. It should be supported by staff vigilance, a robust curriculum, effective reporting systems, appropriate staff training, acceptable use policies and a strong safeguarding culture.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' (KCSIE) requires 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's IT system".*

Therefore, all HET schools should ensure that:

- Filtering and monitoring arrangements are child-centred and risk-based
- Safeguarding, school leadership and IT colleagues work collaboratively
- Concerns are identified, assessed and responded to promptly
- Filtering and monitoring information informs safeguarding practice, staff training and curriculum provision
- Emerging risks, including those associated with artificial intelligence (AI), are regularly considered
- Arrangements are reviewed at least annually and whenever new risks are identified.

We recognise that a filtering system cannot provide a 100% guarantee as online content changes dynamically and new technologies are constantly being developed. It is therefore important to understand that filtering is only one element in a larger strategy for online safety and acceptable use of IT.

It is also important to note that KCSIE 2026 now explicitly recognises AI as an online safeguarding risk.

Schools should remain alert to emerging online risks, including those associated with artificial intelligence (AI). These may include AI-generated content, deepfake images and videos, nudification applications, AI chatbots, misinformation, online manipulation and technology-enabled abuse. Filtering and monitoring arrangements should form part of the school's wider approach to identifying and managing these risks.

3. **Definitions**

- **Abuse** is a form of maltreatment of a child and may involve inflicting harm or failing to act to prevent harm.
- **Artificial Intelligence (AI),** technology capable of generating or manipulating text, images, audio or video, including risks such as deepfakes, nudification tools and AI-generated harmful content.
- **Child** refers to all young people who have not yet reached their 18th birthday. On the whole, this will apply to pupils of our school; however, the policy will extend to visiting children and students from other establishments.
- **Child-on-Child Abuse:** Abuse occurring between children, including bullying, cyberbullying, sexual harassment, sexual violence, harmful sexual behaviour, coercive behaviour and online abuse.
- **DSL** refers to Designated Safeguarding Lead.
- **DDSL** refers to Deputy Designated Safeguarding Lead.
- **Filtering** is a preventative measure that protects users from accessing illegal, inappropriate or potentially harmful online content.
- **HR** in this policy, means Hamwic Education Trust HR.
- **Local Governing Committee** in this policy, where reference is made to the Governing Committee, this means the Local Governing Committee of the school, or the Trust in the case of a school where no Local Governing Committee is present. Where a Governing Committee is not present in a school, or numbers are low, Governors from other schools/partnerships may be used.
- **Monitoring,** the review of user activity on school devices, networks and systems to identify safeguarding concerns, inappropriate behaviour or risks of harm.
- **Online Safety,** the safeguarding and education of pupils and staff when using technology, including the identification and management of online risks.
- **Parent** refers to birth parents and other adults in a parenting role for example adoptive parents, stepparents, guardians, foster carers and kinship carers.
- **School**, when we refer to school if the setting includes a nursery this is included in the definition.
- **Staff** applies to all those working for or on behalf of the school, full-time or part-time, in either a paid or voluntary capacity. This also includes parents and governors.

4. Child-on-Child Abuse

KCSIE 2026 reinforces the expectation that schools recognise, respond to and record child-on-child abuse appropriately, including incidents occurring online. Filtering and monitoring systems are one means by which schools may identify these concerns.

Filtering and monitoring information may identify indicators of child-on-child abuse, including bullying, cyberbullying, prejudiced behaviour, online sexual harassment, harmful sexual behaviour, coercive and controlling behaviour, sharing of indecent images, misogynistic behaviour, and AI-generated or digitally manipulated imagery.
Schools should ensure filtering and monitoring information is considered alongside all other safeguarding information and not in isolation.

5. HET Filtering & Monitoring expectations

HET expect School Leaders, DSLs, and IT staff to work together to ensure every school meets the filtering and monitoring standards made clear in KCSIE and in other relevant DfE documents.

It is important HET staff are clear on the actions they need to take to safeguard children when online or using IT equipment.

Please be aware of these basic expectations we expect of schools around filtering and monitoring:

1. School Leaders and DSLs should understand how filtering and monitoring systems operate, what they do and do not monitor, how alerts are categorised, and any limitations of the systems in use.
2. All School Leaders should receive the alerts from the filtering & monitoring system, or delegate this to another member of the school leadership team.
3. To allow for absence, at least two members of school staff should have access to alerts and reports.
4. HET expect all alerts on the Smoothwall monitor platform to be read and reviewed, changing the status to closed, with a brief note of action, to demonstrate the system is being well managed.
5. HET expect all Level 4 & 5 alerts to be actioned as soon as possible like any other safeguarding concern where a child may be at risk of harm. Appropriate action must be taken and recorded on your safeguarding system (CPOMS or MyConcern).
6. HET expect all Level 3 alerts to be reviewed, with schools using their professional judgement to determine whether recording on CPOMS or MyConcern is necessary.
7. HET expect Level 1 and 2 alerts to be reviewed regularly but advise that ideally this should be done weekly, and daily for any high-risk

pupils. Alerts should be managed through the Smoothwall platform and appropriate action taken where required.

8. The frequency of the review of alerts should be aligned with existing school risk assessments (whole school, Prevent and individual child). All approved users will get instant alerts.
9. Filtering and monitoring should be a standing item at every weekly or fortnightly DSL meeting (regularity will vary school-to-school depending upon size and safeguarding context).
10. Weekly reports containing all alerts must be reviewed, discussed and appropriate actions agreed.
11. DSLs and IT staff are to work together to ensure systems are working effectively in their schools. As an example, this would be a DSL alerting IT that a site needs to be blocked or unblocked.
12. DSLs and IT staff to work together to consider risks around pupils bringing their own devices into school.
13. DSLs to use reports to ensure pupils receive the information and education they need to be safe; this must consider both national safeguarding challenges and trends, alongside the local safeguarding context.
14. DSLs to use reports to ensure pupils receive the information and education they need for topics such as online safety and responsible digital behaviour.

* See the section below (Support from HET) around how to manage your email inbox to separate the different category of alerts.

6. **Filtering system (Smoothwall)**

Filtering system alerts come in three categories set by the system:

1. Danger - The highest importance, shown in red
2. Caution - Shown in orange
3. Advisory - Shown in blue-green

Currently all alerts are received by email. Reports are accessed via the portal; these need to be run manually.

IT support can help schools to manage users. If schools wish to change the staff who receive alerts and have access to the portal, please speak to IT support.

School leaders, DSLs and IT staff should understand the strengths and limitations of the filtering and monitoring systems used within their school. Technical solutions cannot identify every safeguarding concern and may not monitor activity on personal devices, mobile networks, encrypted services or offline content. Schools should ensure these limitations are mitigated through appropriate supervision, staff vigilance, education and wider safeguarding arrangements.

7. **New Online Monitoring system for September 2026 (through Smoothwall)**

Monitoring is looking at and watching what children are doing when they are online. There are three main ways to do this:

1. Physical monitoring (where staff observe pupil screens while they are using them)
2. Internet and web logs.
3. Using a technical monitoring system (**this has been introduced in September 2026 across all HET schools**)

From September 2026, we have introduced a technical monitoring system through Smoothwall. DSLs should be alert to indicators of misogynistic, discriminatory, hateful or abusive content and consider whether alerts present safeguarding concerns requiring intervention and/or education.

Monitoring system alerts come in various categories and set a different level (1-5) for each category.

Some categories included are Bullying, Grooming, Offensive, Oversharer, Sexual Content, Terrorism & Extremism, Violence, Vulnerable Person, etc. and each will have a different definition of the level (1-5).

More information on how these levels are categorised can be found here: Risk Categories – Monitor Help Centre

Any further issues please contact safeguarding@hamwic.org.

8. **Reports**

DSLs should regularly visit the Smoothwall reporting platform:
Reporting (https://portal.smoothwall.cloud/reporting)

There is a filtering dashboard to show you things like top users at risk, top blocked sites, top visited sites, etc. You will also be able to create your own reports to review data about a device and/or user school filtering reports.

Monitor (https://portal.smoothwall.cloud/monitor)
This is the monitoring dashboard to show you how many things were captured, how many transferred into being a safeguarding concern and alert, and the level of the alert.

You will also be able to create your own reports to review data about a device and/or user school monitoring report.

You will also be able to check all the devices that are being monitored at the school.

Regular report checks and reviews are important, and these can be used to give reports to the Governors as well.

9. **Recording pupil filtering and monitoring alerts**

DSLs should consider whether filtering or monitoring alerts indicate wider safeguarding concerns, including child-on-child abuse. This may include online bullying, cyberbullying, online sexual harassment, harmful sexual behaviour, misogynistic behaviour, coercive or controlling behaviour, the sharing of indecent imagery, or the creation, possession or sharing of AI-generated or digitally manipulated images (including deepfakes).

Level 4 and Level 5 alerts flagged by Smoothwall monitor must always be recorded on the school's safeguarding system (CPOMS or MyConcern) and managed through the school's safeguarding procedures, in addition to updating the Smoothwall dashboard.

Level 3 alerts should be reviewed, with schools using their professional judgement to determine whether recording on their safeguarding system is necessary.

Level 1 and Level 2 alerts should be reviewed and managed through the Smoothwall dashboard, with actions recorded within the platform where appropriate.

It is important to remember that information gleaned from logs can be just as important as other sources of safeguarding information; please consider this when deciding whether to record an alert.

DSLs should also consider patterns, repeated low-level alerts and cumulative concerns, recognising that safeguarding risks may emerge over time rather than from a single incident.

The safeguarding category will need to be assessed on a case-by-case basis by the DSL; the following HET categories may be considered:

CPOMS	MyConcern
Cause for Concern: Cause for Concern Online Behaviour	Online - Safety
Child-on-Child: Child on Child Online Child on Child Sexual Harassment	Child on Child Online Abuse Child on Child Sexual Harassment
Harmful Sexual Behaviour: Harmful Sexual Behaviours Online	Harmful Sexual Behaviours Online
Cause for Concern: Cause for Concern Prevent	Extremism and Radicalisation

Exploitation: Child Criminal Exploitation (CCE) Child Sexual Exploitation (CSE)	Child at Risk of Exploitation Indicators of Child Exploitation Child Criminal Exploitation Child Sexual Exploitation
Mental Health: Suicidal Ideation	Mental Health Suicidal Thoughts

10.**Devices loaned to pupils**
Any device loaned to a pupil being educated in a HET school will have filtering & monitoring applied to it, regardless of whether it is being used in or out of school.

Pupils who are given devices to use at home should have signed a Student IT Loan Agreement, alongside their parents and/or carers.

In addition to this, they should have also signed a Pupil Acceptable Use of IT Agreement.

DSLs are to risk assess and action safeguarding concerns from the use of a school device at home in the same way as in-school use.

11.**Staff concerns (filtering only)**
As of September 2026, the Smoothwall monitoring system is only being used to monitor the online activity of pupils.

Any concerns around the actions of staff should only be reviewed and managed by the School Leader and not any other member of the school safeguarding team. Smoothwall staff email alerts should only be accessed by the School Leader. Where School Leaders require advice, they should contact HET HR Team for guidance.

12.**Responsibilities**
It is the responsibility of the School Leader to ensure that their school:

- Has a nominated member of the Senior Leadership Team with responsibility for filtering and monitoring.
- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems.
- Reviews their filtering and monitoring provision at least annually. Schools must keep evidence that the review has taken place and any actions arising from it.
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- Has effective monitoring strategies in place that meet their safeguarding needs.

Whilst HET has overall strategic responsibility for filtering and monitoring, the LGC should seek assurance from the School Leader and DSL, that the school's filtering and monitoring arrangements are effective and that the required standards are being met. Governors should maintain an appropriate awareness of filtering and monitoring and ensure that any necessary support is provided by, or sought from, HET where required. Filtering and monitoring should form a regular part of leaders' reports to the LGC, enabling governors to provide appropriate challenge and oversight.

The Local Governing Committee must:

- Assign one governor to be responsible for making sure filtering and monitoring standards are met.
- Ensure one member of the senior leadership team (SLT) is responsible for overseeing the effectiveness of the school's filtering and monitoring and is their named SLT Lead.
- Ensure the school has appropriate systems in place to regularly and effectively fulfil their Prevent duty.
- Make sure that filtering and monitoring is reviewed at least once per academic year.
- Seek assurance that filtering and monitoring arrangements are effective rather than relying solely on confirmation that systems are in place.
- Receive assurance that:
  - annual filtering and monitoring reviews have been completed
  - actions arising from reviews have been implemented
  - appropriate records are maintained.

DSL's responsibilities include:

- Evaluating risk and acting upon alerts in a timely way.
- Responding to safeguarding concerns identified by filtering and monitoring. Where necessary, liaising with and giving advice and information to pupils, parents, and carers. Signposting to external services as and when required.
- Monitoring reports and alerts should be used to identify concerns relating to AI-generated content, deepfakes, nudification tools, online exploitation and other emerging online risks.
- Ensuring that emerging online safeguarding risks, including AI-generated content, deepfakes and technology-enabled abuse, are considered as part of safeguarding assessments and interventions.
- Using filtering and monitoring information to inform safeguarding risk assessments, curriculum planning, staff training and targeted interventions.
- Ensuring appropriate alerts and actions are recorded on the school safeguarding system (CPOMS or MyConcern).

- Running relevant reports and discussing concerns, information and trends at DSL meetings.
- Working with IT to ensure that filtering works for your school setting and the needs of your pupils.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Making sure all school staff know how to report and record concerns.

IT are responsible for the technical elements such as:

- Maintaining the filtering & monitoring system.
- Maintaining records of routine checks to confirm filtering and monitoring systems are functioning effectively across all internet-connected devices, networks and locations used by the school.
- Regular checks on devices to ensure they are properly configured.
- Working with the DSL to ensure filtering covers any new or local safeguarding context.
- Making sure our filtering & monitoring systems work on new devices and services before they are released to staff and pupils.
- Blocking and unblocking sites following feedback from the DSL and other senior staff.

All HET staff should:

- Understand that filtering and monitoring systems support safeguarding but do not replace professional curiosity or the requirement to report concerns immediately.
- Understand their responsibility in relation to filtering and monitoring as part of their ongoing safeguarding training.
- Know how to report safeguarding and technical concerns, such as if:
  - They witness or suspect unsuitable material has been accessed.
  - They are able to access unsuitable material.
  - They are teaching topics that could create unusual activity on the filtering logs.
  - There is a failure in the software or an 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.
- Know the relevant HET and school-specific policies, processes and procedures and ensure they are followed.
- Understand that they should not share any of their log-in details or passwords with children or other staff or allow a pupil to use their staff device unless closely supervised at all times.

13.**Assurance and Inspection Readiness**
Schools should be able to demonstrate:

- Who is responsible for filtering and monitoring
- How alerts are reviewed, who reviews them and how often they are reviewed
- What actions have been taken
- How concerns are escalated
- Evidence of an annual review; incorporating patterns, trends and actions, as appropriate.
- How alerts and trends have influenced safeguarding practice
- Governor oversight
- Staff training
- Evidence that filtering and monitoring arrangements remain appropriate for the school's safeguarding context
- Evidence that leaders understand the capabilities and limitations of their filtering and monitoring systems.

14. Reviewing your provision

Filtering and monitoring trends should directly inform RSHE, PSHE, online safety education, behaviour interventions, assemblies and staff training. Reviews should involve safeguarding, leadership and IT colleagues to ensure both safeguarding effectiveness and technical functionality are considered.

Each school system needs to be right for your school and meet the needs of pupils and staff. Therefore, any review should take account of:

- The risk profile of your pupils, including their age range and additional needs such as SEND and English as an additional language (EAL).
- Contextual safeguarding influences.
- Risks arising from artificial intelligence and emerging technologies. Filtering and monitoring processes should support the identification of concerns relating to AI-generated imagery, deepfakes, nudification tools, online manipulation and other technology-enabled abuse.
- Lessons learned from safeguarding incidents, local and national safeguarding trends, changes to technology, and feedback from staff where appropriate.
- Teaching requirements e.g. the RHSE and PSHE curriculum.
- Your school's specific use of technology (systems and software).
- What your filtering system currently blocks or allows and why.
- What checks are currently taking place and how resulting actions are handled.

Reviews must be carried out at least once every academic year by the SLT member responsible for filtering and monitoring, supported by the DSL and relevant IT staff. The review should be conducted as a minimum **annually**, or when:

- Emerging technologies, including AI tools and applications, introduce new safeguarding risks or behaviours
- You identify a new safeguarding risk.
- There is a change in your working practice.
- You introduce new technology.
- There are major software updates.
- There are changes to the technical configuration of your network and devices.

A written record of the review, findings, actions taken and any identified development areas must be maintained and made available to governors and HET MS staff upon request.

To make the filtering and monitoring provision effective, the review will inform:

1. Consideration of emerging online risks, including those relating to artificial intelligence and digitally manipulated content.
2. Safeguarding and technology procedures.
3. Roles and responsibilities.
4. Training of staff.
5. Curriculum and learning opportunities.
6. Procurement decisions.
7. How often and what is checked.

Reviewing your provision means you know it is effective against the changing needs and potential risks to your school.

15.**Support from HET MS staff**

Support on understanding obligations around filtering & monitoring can come from both the IT and safeguarding teams at Hamwic. The links below may also be useful.

For further information on the DSL expectations around filtering and monitoring, please contact: safeguarding@hamwic.org.

The IT team can support by:

1. Making sure the right staff receive alerts and have access to the filtering portal.
2. Helping to understand the portal and to run reports.
3. Helping to manage alerts (e.g. email rules so that cautionary and advisory alerts are automatically sent to an email inbox to be reviewed later).
4. Giving assurances to DSLs around the filtering provision in the school.
5. Working with DSLs to make sure the system works in the best way for the school.

16. HET Safeguarding Reviews

The safeguarding team will be reviewing filtering and monitoring as part of the safeguarding ongoing reviews.

17. Link to other HET Policies

- HET Acceptable Use of IT (Staff and Pupils)
- HET Online Safety Policy
- HET Safeguarding and Child Protection Policy
- HET Staff Code of Conduct.
- School Technical Security Policy

18. Useful information and links

1. KCSIE: Keeping children safe in education 2026: September 2026
2. Filtering and monitoring standards for schools and colleges: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK
3. How schools and colleges can meet IT service and digital equipment standards: Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK
4. South West Grid for Learning: Filtering and Monitoring | SWGfL
5. A Guide for education settings and filtering providers: Appropriate Filtering and Monitoring - UK Safer Internet Centre
6. 2025 Appropriate Filtering and Monitoring Definitions: 2025 Appropriate Filtering and Monitoring Definitions Published - UK Safer Internet Centre
7. Appropriate Filtering for Education settings: Appropriate Filtering - UK Safer Internet Centre
8. Online Safety Self-Review Tool for Schools: 360 Degree Safe - Online Safety Review Tool | SWGfL
9. Smoothwall Help Centre: Smoothwall Help Centre
10. Smoothwall Monitor Help Centre: Monitor Help Centre