Meeting digital and technology standards in schools and colleges (DfE)

This checklist has been formatted to align with the DfE standards September 2025

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff

Please note in accordance with KCSIE - The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty 31. The Prevent duty Departmental advice for schools and childcare providers and Home Office Statutory guidance: Prevent duty guidance.

October 2024 updates are indicated in yellow

Please RAG Rate your checklist as follows

Red – requires immediate attention (by end of half term)
Amber – actions to be completed within an identified timescale
Green – complete - no action needed

RAG rate the action column

			Action By whom/when by	Evidence
A		**You should identify and assign roles and responsibilities to manage your filtering and monitoring systems**		
	A1	Have governors or proprietors identified and assigned a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met?	Green	
	A2	Have governors or proprietors identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?	Green	Fully compliant - DCC are the third party
	A3	Does the Senior Leadership Team understand that they are responsible for: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports	Green	Fully compliant - With support from BCCET
	A4	Has the SLT ensured that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Green	Fully compliant - Staff meetings, safeguarding policies and training
	A5	Are arrangements in place for governors or proprietors, SLT, DSL and IT service providers to work closely together?	Green	Fully compliant - IT technician, support from Trust, governors updated around filtering and monitoring
	A6	Does the DSL take 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? • Ensuring compliance with KCSIE	Green	Fully compliant - HT and DHT get automated emails from Smoothwall and Senso and action these
	A7	Does the IT service provider have technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Green	Fulfilled

	A8	Has the IT service provider worked with the senior leadership team and DSL to: • procure systems • identify risk • carry out reviews • carry out checks	Green	
	A9	Does the SLT assess how your students' risk profile could inform your approach to filtering and monitoring, considering things such as their age, if they have any special education needs and disabilities (SEND) and whether they have English as an additional language (EAL)	Green	Fully compliant - All students are filtered and monitored at all times through our systems
B		**You should review your filtering and monitoring provision at least annually**		
	B1	Have governing bodies and proprietors ensured that filtering and monitoring provision is reviewed at least annually, to identify the current provision, any gaps, and the specific needs of your pupils and staff?	Green	Fully compliant - Systems are tight and in place and meet the needs of school
	B2	Are reviews conducted by SLT, DSL, and the IT service provider and involve the responsible governor?	Amber Ensure governors meetings document an annual review	IT team On an annual basis we check that the correct staff are set to receive the filtering alerts.
	B3	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?	Amber Online safety review to be shared with governors	In place bur needs reviewing and sharing with governors
	B4	Does the review cover all required elements (as a minimum)?	Green	Fully compliant
	B5	Have reviews informed:	Green	Fully compliant
		• 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		
	B6	Does the review ensure that checks of the system have been carried out? Test Your Internet Filter (UKSIC / SWGfL)	Green	Fully compliant - Tested daily

C		Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning		
		Technical requirements to meet the standard		
		Go here to see self-certified provider statements		
	C1	Is your filtering provider • a member of 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)	Green	Fully compliant
	C2	Is the school's filtering operational and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection • bring your own devices (BYOD) • Apps • generative AI tools	Green	Fully compliant – all devices are filtered through Smoothwall
	C3	Does the filtering system: • filter all internet feeds, including any backup connections • be age and ability appropriate for the users, and be suitable for educational settings • handle multilingual web content, images, common misspellings and abbreviations • identify new 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	Green	Fully compliant
	C4	Has a technical monitoring system been applied to devices using mobile or app content?	Green	
	C5	Does the filtering system identify: • device name or ID, IP address, and where possible, the individual • the time and date of attempted access • the search term or content being blocked	Green	Fully compliant
	C6	Are there any additional levels of protection for users beyond the filtering service, such as SafeSearch or a child-friendly search engine?	Green	Fully compliant
	C7	Have staff been given guidance on how to provide effective supervision of students using devices? • All staff should conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision.	Green	Supervision in all lessons, staff had training in staff meeting

	C8	Are staff aware that they should make a report when: • 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	Green	Fully compliant
	C8	Does the school meet the Broadband Internet Standards?	Green	Fully compliant
	C9	Does the school meet the Cyber Security Standards?	Green	Fully compliant
	C10	Have all staff who use the school's IT Network had annual Basic Cyber Security/E-safety Training??	Green	Fully compliant
	C11	Has a least one governor attended a Basic Cyber Security training session?	Green	Fully compliant

D		**You should have effective monitoring strategies that meet the safeguarding needs of your school or college**		
	D1	Does the monitoring system review user activity on school and college devices effectively? (For example, does it pick up incidents urgently, through alerts or observations, allowing prompt action to be taken; and is the response recorded?	Green	Fully compliant
	D2	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?	Green	Fully compliant
	D3	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?	Green	
	D4	Has the DSL had training to ensure that their knowledge is current?	Green	
	D5	Have IT staff had training to ensure that their knowledge is current?	Green	Fully compliant
	D6	Are monitoring procedures reflected in the school's Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices?	Green	
	D7	If the school has technical monitoring system, has a data protection impact assessment (DPIA) been completed? A data protection impact assessment can be found here	Amber	Managed by DPO, Sarah Burns
	D8	If the school has a technical monitoring system, has a review of the privacy notices of third party providers being undertaken?	Amber	Managed by DPO, Sarah Burns
		Model privacy notices can be found here		

Filtering and Monitoring

Useful links and resources

Department for Education

Keeping Children Safe In Education (DfE)
Meeting digital and technology standards in schools and colleges (DfE)
Broadband internet standards for schools and colleges (DfE)
Cyber security standards for schools and colleges (DfE)
Data protection policies and procedures (DfE)

Home Office

The Prevent duty: safeguarding learners vulnerable to radicalisation (Home Office)

Information Commissioner's Office

Data Protection Impact Assessment (DPIA) (ICO)

National Cyber Security Centre

Cyber security training for school staff

UK Safer Internet Centre

Test Your Internet Filter (UKSIC / SWGfL)
Filtering provider responses - self-certified by service providers (UKSIC)
A Guide for education settings and filtering providers (UKCIS)
Establishing appropriate levels of filtering (UKSIC)
Online safety in schools and colleges: questions from the governing board (UKCIS)

Digital Resilience

HeadStart Online Digital Resilience Tool (HeadStart Kernow)