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)

London Grid for Learning (LGfL)

Online Safety Audit (LGfL)

South West Grid for Learning (SWGfL)

Online Safety Review (360Safe) (SWGfL)

National Cyber Security Centre

Cyber security training for school staff

UK Safer Internet Centre

2023 Appropriate filtering and monitoring definitions published (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)

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

(NB Although the DfE standards are not numbered, I have done so here to help with clarity.)

			Yes/No	Comment
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?		
	A2	Have governors or proprietors identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?		
	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		
	A4	Has the SLT ensured that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns		
	A5	Are arrangements in place for governors or proprietors, SLT, DSL and IT service providers to work closely together?		
	A6	Does the DSL should 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?		
	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		
	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		
B		**You should review your filtering and monitoring provision at least annually**		
		Go to Review Questions		
	B1	Have governing bodies and proprietors ensured that filtering and monitoring provision is reviewed at least annually, to to identify the current provision, any gaps, and the specific needs of your pupils and staff?		
	B2	Are reviews conducted by SLT, DSL, the IT service provider and involve the responsible governor?		
	B3	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?		
	B4	Does the review cover all required elements (as a minimum)?		
	B5	Have reviews informed:		
		• 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?		
		Go to Checks on filtering		
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)		
	C2	Is the school's filtering operational and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection		
	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 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		
	C4	Has the provider confirmed that filtering is being applied to mobile and app content?		
	C5	Has a technical monitoring system been applied to devices using mobile or app content?		
	C6	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		
	C7	Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?		
	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		
	C9	Does the school meet the Broadband Internet Standards?		
	C10	Does the school meet the Cyber Security Standards?		
		Two important elements of the Cyber Security Standards are that all staff who can access the IT Network have Basic CyberSecurity Awareness Training annually; and that at least one governor access this training.		
		Cyber Security Training from the National Cyber Security Centre can be found here as a PPT slide deck and a self-learn video		
	C11	Have all staff who use the school's IT Network had annual Basic Cyber Security Training?		
	C12	Has a least one governor attended a Basic Cyber Security training session?		
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?		
	D2	Has the governing body or proprietor supported the SLT to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college?		
	D3	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?		
	D4	Is it clear to all staff how to deal with these incidents and who should lead on any actions?		
	D5	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?		
	D6	Has the DSL had training to ensure that their knowledge is current?		
	D7	Have IT staff had training to ensure that their knowledge is current?		
	D8	Does the school's monitoring technology apply to mobile devices or content used in apps?		
	D9	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?		
	D10	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		
	D11	If the school has technical monitoring system, has a review the privacy notices of third party providers being undertaken?		
		Model privacy notices can be found here		