Sample DSL Annual Filtering & Monitoring Audit 2025-2026

Meeting digital and technology standards in schools and colleges (DfE)
(NB Although the DfE standards are not numbered, they are numbered here to help with clarity.)

Recommendations:
For filtering and monitoring to be effective it should meet the needs of your pupils and staff and reflect your specific use of technology while minimising potential harms.
To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision, **at least annually.**
Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies and stakeholders have assurance that systems are working effectively and meeting safeguarding obligations.

	DSL Annual Filtering & Monitoring Audit 2025-2026	Yes / No	Comments
A	**You should identify and assign roles and responsibilities to manage your filtering and monitoring systems.**		
A1	Have governors or stakeholders identified and assigned a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met?	Yes	Mark Thornley Linked to the safeguarding governor.
A2	Have governors or stakeholder identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?	Yes	**BSICT** – we a line all our support with [DFE Digital and technology standards](#)
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	Yes	Reported to governors every term and standing item in staff development meetings and staff briefings
A4	Has the SLT ensured that all staff: • understand their role • are appropriately trained • follow policies, processes, and procedures • act on reports and concerns	Yes	**BSICT** produced a KCSIE Resource pack that included CPD for schools to deliver to staff
A5	Are arrangements in place for governors or stakeholders, SLT, DSL and internet service providers (ISP) to work closely together?	Yes	**BSICT** – Safeguarding team, PPR, cluster meetings, Governor trainings, drop ins.
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?	Yes	**BSICT** helps with safeguarding concerns. Safeguarding team. BSICT Onsites do half termly checks.
A7	Does the ISP have technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Yes	**BSICT** calls for ad hoc and regular monitoring, automated security alerts and action taken as required.
A8	Has the IT service provider worked with the senior leadership team and DSL to: • procure systems • identify risk • carry out reviews	Yes	**BSICT** – Safeguarding team, PPR and project testing schools.

		• carry out checks		
B		**You should review your filtering and monitoring provision at least annually.**		
	B1	Have governing bodies and stakeholders 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?	Yes	Yes, added to autumn policy review. Safeguarding briefing focus on filtering and monitoring in Autumn.
	B2	Are reviews conducted by SLT, DSL, the Internet Service Provider (ISP) and involve the responsible governor?	Yes	Half termly checks by onsite technician. This is feedback to responsible governor.
	B3	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?	Yes	Part of the Head Teacher termly report
	B4	Does the review cover all required elements (as a minimum)?	Yes	
	B5	Have reviews informed:	select	
		• related safeguarding or technology policies and procedures	Yes	
		• roles and responsibilities	Yes	
		• training of staff	Yes	
		• curriculum and learning opportunities	Yes	Digital citizenship emphasis in our curriculum.
		• procurement decisions	Yes	
		• how often and what is checked	Yes	
		• monitoring strategies	Yes	
	B6	Does the review ensure that checks of the system have been carried out?	select	Termly checks by ICT technician
C		Y**our filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning**		
	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)	Yes	
	C2	Is the school's filtering operational and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection	Yes	**BSICT** - 2 levels of filtering: **School Wi-Fi** for all school devices only. **Guest Wi-Fi** for any non-school devices and guest users
	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	Yes	**BSICT** – Nov2023-2024: Firewall - Sophos Fastvue – Filtering & monitoring **Nov2024 – Nov 2025:** Firewall – WatchGuard Filtering & Monitoring - Lightspeed
	C4	Has the provider confirmed that filtering is being applied to mobile or app content?	Yes	

	C5	Has a technical monitoring system been applied to devices using mobile or app content?	Yes	
	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	No	**BSICT** – on Microsoft devices both adults and pupils log on with their own accounts. On mobile devices pupils are issued with the same devices to enable. Alerts contain an overview of time, date and attempted content accessed.
	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?	Yes	**BSICT** - Specific pupil filtering policy SafeSearch applied on all users accessing the internet
	C8	Are staff aware that they should <mark>make a report when:</mark> • 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	Yes	**BSICT** produced a KCSIE Resource pack that included CPD for schools to deliver to staff. This was delivered.
	C9	[Does the school meet the Broadband Internet Standards?](#)	Yes	Our ISP is **Bolton Schools ICT**
	C10	[Does the school meet the Cyber Security Standards?](#)	Yes	Our ISP is **Bolton Schools ICT**

*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?	Yes	Smart Log Spring 2 training
	C12	<mark>Has a least one governor attended a Basic Cyber Security training session?</mark>	No	
D	**You should have effective monitoring strategies that meet the safeguarding needs of your school**			
	D1	Does the monitoring system review user activity on school devices effectively?	Yes	Chromebooks are numbered and issued to children to help monitor what children are accessing
	D2	Has the governing body or stakeholders 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?	Yes	
	D3	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?	Yes	**BSICT** alerts instant and reported to the school DSL
	D4	Is it clear to all staff how to deal with these incidents and who should lead on any actions?	Yes	Follow the online safety flowchart

D5	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?	Yes	
D6	Has the DSL had training to ensure that their knowledge is current?	Yes	Advanced DSL safeguarding training (Bolton ICT are creating a video to provide further training)
D7	Have IT staff had training to ensure that their knowledge is current?	Yes	
D8	Does the school's monitoring technology apply to mobile devices or content used in apps?	Yes	
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?	Yes	**BSICT** – have a set of sample AUPs for staff, visitors and age-appropriate pupil Technology agreements
D10	If the school has technical monitoring system, has a data protection impact assessment (DPIA) been completed?	Yes	**BSICT** – updated our DPIA
D11	If the school has technical monitoring system, has a review the privacy notices of third-party providers being undertaken?	Yes	Privacy notices in place, including DPIAs for apps and wesites

Any other comments Has there been any trends regarding alerts? Has there been any trends regarding content searched that has flagged an alert?
No trends – whatsapp/social media groups use outside of school causes the most concern. Re launch of the 4Cs and conduct emphasised.

References used to produce this Sample Annual Audit

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- 2023 – Andrew Hall | Safeguarding Info
- Test Your Internet Filter (UKSIC / SWGfL)
- Data protection impact assessments | ICO
- Data protection in schools - Data protection policies and procedures - Guidance - GOV.UK (www.gov.uk)