School Name: WALTER HALLS PRIMARY SCHOOL

Date: SEPTEMBER 2024

Filtering and Monitoring Checklist

Useful links and resources	
Department for Education	Keeping children safe in education - GOV.UK (www.gov.uk) Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Meeting digital and technology standards in schools and colleges - Broadband internet standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Data protection in schools - Data protection policies and procedures - Guidance - GOV.UK (www.gov.uk)
Home Office	The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk)
Information Commissioner's Office	Data protection impact assessments | ICO
London Grid for Learning (LGfL)	Broadband and Beyond - Online Safety Audit (lgfl.net)
South West Grid for Learning (SWGfL)	Online Safety Self-Review Tool for Schools | 360safe
National Cyber Security Centre	Cyber security training for school staff - NCSC.GOV.UK
UK Safer Internet Centre (UKSIC / SWGfL)	2023 Appropriate filtering and monitoring definitions published - UK Safer Internet Centre Test Your Internet Filter | SWGfL Test Filtering Filtering Provider Responses - UK Safer Internet Centre A Guide for education settings and filtering providers (UKCIS) Appropriate Filtering and Monitoring - UK Safer Internet Centre Appropriate Filtering - UK Safer Internet Centre Online safety in schools and colleges: questions from the governing board - GOV.UK (www.gov.uk)
Digital Resilience	Digital Resilience : Headstart Kernow

Name Members of staff responsible to:

Monitor software and communicate concerns with DSLs and SLT	Smoothwall / Alex Epton
Work with schools IT to ensure software is working correctly and updated	Alex Epton / Gail Holmes
Report any technical issues to school IT	Alex Epton / Belinda O'Connor
Work with schools IT to run annual checks to ensure systems are working	Alex Epton / Belinda O'Connor
Establish tracking /monitoring systems so it is clear which user is using which device	Gail Holmes / Emma Beardah
This can include labelling devices (visually and on the IT network)	Gail Holmes / Emma Beardah
Creating timetables for use	Abby Cottam / Emma Beardah

Creating user logs so that any concerns can be traced to user activity	Abby Cottom / Emma Beardah
Ensure staff are aware of their roles and responsibly in relation to monitoring	Gail Holmes / Emma Beardah
Update policies in school to reflect these changes (behaviour policy, safeguarding, appropriate use of internet, teaching and learning) where appropriate	Gail Holmes / Emma Beardah
Recognise no system is 100% and staff also actively monitor online activity and are aware of potential short falls in software systems (i.e use of hot spots)	Gail Holmes / Emma Beardah
Ensure stake holders such as governors and parents are aware of the systems in place	Emma Beardah
Make arrangements for staff induction	In place – Gail Holmes DSL
Make arrangements for visitor use of the internet (i.e supply teachers)	In place – Gail Holmes DSL

Checklist:

			Yes/ No	Comment
A		**You should identify and assign roles and responsibilities to manage** your filtering and monitoring systems	Yes	In place from 2021/22, use of Smoothwall and assigned roles on safeguarding team
	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?	Yes	Emma Beardah - Headteacher Gail Holmes – Safeguarding Alex Epton – SBM & Governor Abby Cottam – Computing lead
	A2	Have governors or proprietors identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?	Sept '23	See Schools IT Filtering and Monitoring responsibility docs.
	A3	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	In place 2021/22 and reviewed 2023
	A4	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	In place 2021/22 and reviewed 2023
	A5	Are arrangements in place for governors or proprietors, SLT, DSL and IT service providers to work closely together?	Yes	See Schools IT Filtering and Monitoring responsibility docs.
	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	Yes	See Schools IT Filtering and Monitoring responsibility docs.

		• 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	Yes	Schools IT make requested changes to the school filtering approved by the head teacher. Schools IT look at any issues raised and escalate to the solution provider where necessary. Schools IT keep a log of all changes requested and Head Teachers sign off all changes requested
	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		Schools IT evaluate and recommend filtering and monitoring solutions to meet requirements. For NST schools these include: • https://www.smoothwall.com/education/monitor/ • https://www.securus-software.com/ • https://senso.cloud/gb/safeguard-cloud-online-monitoring-and-safeguarding/ Schools IT review systems and software as appropriate Schools IT ensure that filtering and monitoring software is running effectively on all machines The SLT/ DSL can access reports and alerts through the software and monitor any inappropriate usage.
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?		Governors ensure provision is reviewed annually during the Autumn Term in line with revised KCSIE guidance and in preparation for budget decisions in the Spring Term. Annual health checks are undertaken by Schools IT during the Spring Term to include filtering and monitoring arrangements ensuring software is working effectively.
	B2	Are reviews conducted by SLT, DSL, the IT service provider and involve the responsible governor?		Checklist is reviewed by Governors in the Autumn Term Full Governing Body meeting
	B3	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?		Filtering reports showing the websites blocked and accessed by students are reviewed weekly by Schools IT to ensure that the filtering is functioning. The frequency of these reports can be changed and school email addresses added as recipients of the reports. Monitoring solutions should be configurable to send scheduled overview reports that do not contain personal information but show a summary of what the software is capturing. These reports can be sent to the school and

				used as evidence that the software is doing its job.
	B4	Does the review cover all required elements (as a minimum)?		In place
	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		First review September 2023 Second review September 2024
	B6	Does the review ensure that checks of the system have been carried out?		Schools IT test all aspects of the system as part of the annual health check to ensure it is loaded correctly - schools must check software and report any concerns
		Go to Checks on filtering		Schools IT test filtering system as part of the annual health check.
C		**Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning**		Smoothwall In place
		Technical requirements to meet the standard		Smoothwall - See provider responses.
		Go here to see self-certified provider statements		See provider responses
	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	We use Smoothwall who are • 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	Yes	Direct internet access is blocked and can't be bypassed at device level.
	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	Schools based machines are all protected effectively . However school is aware of potential risks if users use personal hotspots to access the internet which do not necessarily have the same level of protection. Staff are vigilant regarding this risk, and it is only used when absolutely necessary. Pupils are not permitted to bypass the system.

	C4	C4 Has the provider confirmed that filtering is being applied to mobile and app content?	Yes	See provider responses.
	C5	Has a technical monitoring system been applied to devices using mobile or app content?	Yes	See provider responses.
	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	Yes	Identifying individuals requires a user to log onto devices with their own account and not generic/shared ones. On shared devices like iPads where a user doesn't log into a device it is not possible to identify the individual user but it is possible to identify the machine so school take care to identify the user access to each machine by establishing a school based system for allocating devices and monitoring use. This may include labelling devices, timetables and a paper user log
	C7	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	Google SafeSearch is enforced on all machines
	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	Yes	In place from 2021-22 academic year. Briefing reminders and monitoring in place. Part of annual safeguarding CPD for all staff and part of induction for new staff
	C9	Does the school meet the Broadband Internet Standards? Meeting digital and technology standards in schools and colleges - Broadband internet standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)		Schools IT advises school prior to their most recent contract renewal of the latest standards (these advise primary schools have a minimum 100Mbps download and 30Mbps upload speed). We take a decision based on increased cost. However we recognise that a slow connection risk less reliable service. Schools IT review availability monthly for FTTP which is a more cost-effective way to meet the recommendations. **Any schools on FTTC connections do not meet these standards.**

	C1	Does the school meet the Cyber Security Standards? Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Two important elements of the Cyber Security Standards are that all staff who can access the IT Network have Basic Cyber Security 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 Cyber security training for school staff - NCSC.GOV.UK		Schools are protected by hardware firewalls that are updated and maintained by their internet service provider. Windows devices are also configured with a software firewall for use on untrusted networks. Devices are not left with default passwords and are secured with a minimum 6 character password on their initial configuration. Password policies are in place and passwords audited and potential issues raised with schools. Standard user accounts do not have administrative access. Multi-factor authentication is enforced for Office 365 staff accounts.
	C1	Have all staff who use the school's IT Network had annual Basic Cyber Security Training?		All staff complete NCSC training (C10) Cyber security training for school staff - NCSC.GOV.UK
	C1	Has a least one governor attended a Basic Cyber Security training session?		SBM, Alex Epton, is also governor
D		**You should have effective monitoring strategies that meet the safeguarding needs of your school or college**		Monitoring software which will detect and alert designated school staff on potential safeguarding issues is **a requirement**.
	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?		Schools that have any of the below solutions, have a solution that can be configured to meet the requirements. https://www.smoothwall.com/education/monitor/ https://www.securus-software.com/ https://senso.cloud/gb/safeguard-cloud-online-monitoring-and-safeguarding/ Schools It ensure that the monitoring system and alerts are set up effectively.
	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?		Governors discuss this aspect and review compliancy and culture as part of the Autumn Term Governing body meeting
	D3	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?		Smoothwall is configured to email immediate alerts when triggered as well as displaying this information when logged into the system. The safeguarding team receive these alerts.
	D4	Is it clear to all staff how to deal with these incidents and who should lead on any actions?		Clear escalation in place through the safeguarding team and SLT/Phase leaders
	D5	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?		Yes – they are the first point of contact

	D6	Has the DSL had training to ensure that their knowledge is current?		Yes – fully in place since 2021-22 academic year
	D7	Have IT staff had training to ensure that their knowledge is current?		IT staff are trained on the systems used within school. Updates and knowledge are also shared through team meetings. Vendors provide updates via email and meetings.
	D8	Does the school's monitoring technology apply to mobile devices or content used in apps?		All devices that require monitoring will require the monitoring solution client installing on each device.
	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 – in place
	D1	If the school has technical monitoring system, has a data protection impact assessment (DPIA) been completed?		This is actioned by school and the DPO
		A data protection impact assessment can be found here Data protection impact assessments | ICO		This is actioned by school and the DPO
	D1	D11 If the school has technical monitoring system, has a review the privacy notices of third party providers being undertaken?		This is actioned by school and the DPO
		Model privacy notices can be found here Data protection in schools - Data protection policies and procedures - Guidance - GOV.UK (www.gov.uk)		