SPHERE FEDERATION

Scholes (Elmet) Primary
St James' CE Primary
Moortown Primary

Meeting Digital and Technology Standards

Meeting digital and technology standards in schools and colleges (DfE) Sphere Federation		
		comment
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems		
	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?	CW as Federation DSL (KH & NB in other schools) & PW to support
	Have governors or proprietors identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?	Sphere Federation work alongside Adept as ICT support (SQ, HoS, PW to liaise with them alongside HoF)
	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	guidance followed from KCSIE and other policies
	Has the SLT ensured that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	staff follow guidance within several policies including: - Code of Conduct - Safeguarding and CP - KCSIE - GSWP - online safety (acceptable use) CPD
	Are arrangements in place for governors or proprietors, SLT, DSL and IT service providers to work closely together?	evidence in GB minutes; GB visits; job descriptions; contract/agreement with Nextgen and previous provider, Adept
	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?	CW as Federation DSL (KH & NB in other schools) & PW (DDSL @ Moortown) to support
	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
	Has the IT service provider worked with the senior leadership team and DSL to: • procure systems • identify risk • carry out reviews • carry out checks	reviews and check are done regularly internally and any issues raised with Nextgen
You should review your filtering and monitoring provision at least annually		

	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?	GB minutes; GB visits - DSL review annually alongside Governor responsible for safeguarding and filtering. Records kept.
	Are reviews conducted by SLT, DSL, the IT service provider and involve the responsible governor?	yes
	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?	actioned from 2024/25 onwards - this has been done previously but not formally recorded for reference
	Does the review cover all required elements (as a minimum)?	yes
	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	see above
	Does the review ensure that checks of the system have been carried out?	yes
Checks on Filtering		
	Has the system (or any part of it) been tampered with, changed or turned off?	no
	Do the checks cover: • school owned devices and services, including those used off site • geographical areas across the site • user groups, for example, teachers, pupils and guests	Yes – SWGFL checks are regularly carried out by senior leaders – checking iPads, staff laptops and pupil laptops
	Is a log made of the checks?	yes
	Are the following elements of the check recorded: • when the checks took place • who did the check • what they tested or checked • resulting actions	yes
	Do all staff know how to report and record concerns?	yes
	Are new devices and services checked to ensure that filtering and monitoring systems work before releasing them to staff and pupils?	yes
	Have blocklists been reviewed and are they modified in line with changes to safeguarding risks	yes
	Has the filtering system been checked using the SWGfL's testing tool for: • illegal child sexual abuse material • unlawful terrorist content • adult content	yes
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning		
Technical requirements to meet the standard		
	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
	Is the school's filtering operational and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection	evidence when anyone logs in or sites blocked.
	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	filtering needs to be in different languages - eg Urdu/Punjabid/Farsi

	• 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	
	Has the provider confirmed that filtering is being applied to mobile and app content?	evident when trying to log in
	Has a technical monitoring system been applied to devices using mobile or app content?	
	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
	Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?	Safesearch
	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	CPD covering aspects of KCSIE which is relevant to all staff and any other policies (September 2023)
	Does the school meet the Broadband Internet Standards?	yes
	Does the school meet the Cyber Security Standards?	yes
	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	
	Have all staff who use the school's IT Network had annual Basic Cyber Security Training?	All staff have completed basic Cyber security awareness – scheduled to repeat this
	Has a least one governor attended a Basic Cyber Security training session?	Chair of Governors has this as an action for this term
You should have effective monitoring strategies that meet the safeguarding needs of your school or college		
	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?	Incidents are picked up urgently and addressed - responses need to be recorded
	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?	yes
	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?	these are picked up by the HoS or Federation DSL (CW)
	Is it clear to all staff how to deal with these incidents and who should lead on any actions?	all staff are compliant in following policies and regular reminders are incorporated into CPD and weekly briefings
	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?	followed up by HoS or DSL and any concerns recorded on CPOMS all training is up to date
	Has the DSL had training to ensure that their knowledge is current?	yes
	Have IT staff had training to ensure that their knowledge is current?	n/a – external company used
	Does the school's monitoring technology apply to mobile devices or content used in apps?	filters are checked on iPads aswell as other school devices
	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?	Acceptable Use is in place and signed by all staff and governors aswell as pupils