Luston and Shobdon Community Primary Schools Federation including Luston Nursery

Filtering and Monitoring Policy

Last reviewed	**31 January 2024**
Renewal due	**31 January 2025**

ROLES AND RESPONSIBILITIES		
Day to Day Management (DSL and IT service provider)	• Procure systems • Identify risk • Carry out reviews • Carry out checks	Executive Headteacher: Mary Freeman Head of Schools: Georgina Morgan, Kim Kilby Sitech Support Ltd: Simon Eades
Day to Day Management (DSL)	• Filtering and Monitoring Reports • Safeguarding Concerns • Checks and filtering to monitoring system	DSL team: Mary Freeman, Georgina Morgan, Rhiannon Thomas, Elizabeth Jones
Day to Day Management SItech Support Ltd	• Maintaining the filtering and monitoring system • Providing filtering and monitoring reports • Checking the system or completing actions following any concerns	Sitech Support Ltd

ROLES AND RESPONSIBILITIES		

Day to Day Management (SLT)	• Buying-in the filtering and monitoring system the school use
	• Documenting what is blocked or allowed, and why
	• Reviewing the effectiveness of provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded
	• Overseeing reports
	• Making sure staff:
	  ○ Understand their role
	  ○ Are trained appropriately
	  ○ Follow policies, processes and procedures
	  ○ Act on reports and concerns
		Executive Headteacher: Mary Freeman
		Head of School: Georgina Morgan (Shobdon), Kim Kilby (Luston)
		Computing Lead: Beccy Walker
		
		Support from Sitech Support ltd where required

ROLES AND RESPONSIBILITIES		

Day to Day Management (all staff)	Everyone should be clear on:
	• The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens
	• How to report safeguarding and technical concerns, such as if:
	  ○ They witness or suspect unsuitable material has been accessed
	  ○ They are able to access unsuitable material
	  ○ They are teaching topics that could create unusual activity on the filtering logs
	  ○ There is a failure in the software or an 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
		All teaching staff, teaching assistants, wrap around care staff and lunch supervisors

Day to Day Management (Governing Board)	Has overall strategic responsibility for filtering and monitoring. They will need assurance from you that your school is meeting the standards and they need to be aware of what's going on.	Governing body Safeguarding governor lead: Adam Scott

QUESTION	ANSWER	NEXT STEPS/ACTIONS
What is the risk profile of your pupils? E.g.: ○ Their age range ○ Pupils with special educational needs and disabilities (SEND) ○ Pupils with English as an additional language (EAL)	• Ages 4-11 Luston: 27 children on SEND register, 0 EHCPs 5 children with EAL Shobdon: 16 children on SEND register, 1 EHCP 0 children with EAL	• Termly checks on pupil iPads to make sure filtering systems are still in place and effective • Use of Mosyle Class Manager to monitor usage
Does your filtering and monitoring system adhere to the technical requirements? (get your checklist of the requirements here)	See below	

What does your filtering system currently block or allow, and why?	Our schools' Internet connection is filtered by a product called **Securly;** details can be found at www.securly.com. It is a fully cloud-based filtering service that requires no additional hardware located at the school site or software installed onto devices. It operates at network level across all hardware. It is multi-lingual and also filters encrypted (https) traffic. Securly has been a member of the Internet Watch Foundation since 1st March 2016 and is a member of the Counter-Terrorism Internet Referral Unit list. Securly, by default, blocks access to the following content. • Discrimination • Drugs/Substance abuse • Extremism • Gambling • Malware/Hacking • Pornography • Piracy and Copyright Theft • Self-Harm • Weapons and Violence Securly filters all Corporate devices, used by staff and pupils. Guest devices are filtered by the schools Fortigate firewall, logs are produced using Fastvue. Securly will automatically send alerts to a separate school email mailbox which designated staff members have access to. Designated school staff are able to monitor alerts 24/7 if required. The alert message contains information regarding the block and identifying who did this, what the block entailed as well as the date and time.	

QUESTION	ANSWER	NEXT STEPS/ACTIONS
What limitations are there to your filtering system? How will you mitigate them?	Continuing rapid development of APPs and new harmful terminology and technology.	Keep staff and parents up to date with changes to online safety using the National Online Safety #WakeUpWednesday
How do you know your filtering and monitoring system meets the needs of your school? (Use your Prevent risk assessment to help you decide what's appropriate for your school)	Recommended by our IT service– see Securly info above.	
What outside safeguarding influences impact your school? E.g. county lines	County Lines Rural area encourages more online communication amongst pupils.	
Are there any relevant safeguarding reports that impact your filtering and monitoring?	KCSIE 2023	
What is the digital resilience of your pupils? • This means whether your pupils have the knowledge and skills to make decisions online that keep themselves safe, and whether they know what to do if they come across something that's wrong	Children are taught to report to an adult if they come across something of concern. There have been no such reports in the last 2 academic years. If a child was to report a concern, the school would immediately contact IT support to block the website.	

QUESTION	ANSWER	NEXT STEPS/ACTIONS
Are you clear on your teaching requirements, for example, your RHSE and PSHE curriculum?	The school has a clear computing and RSHE schedule of learning.	Subject leads for RSHE and Computing to monitor
Does your school outline any specific uses of technologies? E.g. do you allow staff and/or pupils to 'Bring Your Own Device' (BYOD)?	Acceptable Use Policy Staff code of conduct E-safety policy Staff do not use personal devices on the school system.	
What related safeguarding or technology policies do you have in place?	Prevent Safeguarding and Child Protection Policy E-safety Policy Data Protection Policy	
What checks are currently taking place? How do you handle any resulting actions?	Securly monitoring Fortigate Monitoring Mosyle DNS monitoring EHT follows up with update to staff, assembly information to pupils (in an age appropriate way) and immediate action	

Filtering and monitoring checks

CHECKS	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose? You can signpost your IT service provider to South West Grid for Learning's (SWGfL) testing tool.	07/12/23	Sitech Support Ltd	Termly meetings with Sitech to monitor
Is the system running and working?	YES 07/12/23	Sitech support Ltd	Ongoing monitoring from all staff
Have we checked that our filtering and monitoring system works on: • All devices • New devices and services before they're given to staff or pupils	YES	Sitech Support Ltd	Termly meetings with Sitech to monitor
Have we reviewed the list of blocked sites on our network? Is this list still accurate/does it reflect any changes to safeguarding risks?	Blocked sites include: Manually blocked	Sitech Support Ltd	
Does our filtering system adhere to the requirements? (Get your checklist of the requirements here)	Yes	SItech Support Ltd	

CHECKS	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Does our monitoring system adhere to the requirements? (Get your checklist of the requirements here)	Yes	Sitech Support Ltd	

Monitoring strategy

APPROACH	POINTS TO CONSIDER
Physical monitoring (Where staff monitor pupils' screens while they're using them)	Use this approach where: • Your risk assessment(s) suggests **low risk** • You have staff who can directly supervise pupils 1-to-1 whilst using technology Consider that: • It's difficult to physically monitor any independent use of technology • It can be resource intensive • It is less effective across a larger group, or a group using mobile devices • Students often adapt screen behaviour to avoid monitoring • Some devices cannot be monitored using any other strategy other than physical monitoring, e.g. taking videos/images on mobile devices or cloud storage But it is easier to intervene immediately where an issue arises, and you can use it as a teaching opportunity in the moment.
Internet and web access (Where schools can identify and intervene where someone has accessed or searched for something concerning. This is done by monitoring logfile information, which shows which individuals have accessed certain sites or used certain search terms)	Consider: • That you'll need to assign someone with the responsibility to analyse the logfile information ○ This will require time and specialist technical and/or safeguarding knowledge to analyse, as these reports can be difficult to understand • How frequently these logfiles are updated by your provider • How you can regularly review these logfiles, analyse them and prioritise any alerts • That your logfile information needs to be able to identify individual users so you can intervene • That you must act on any information that indicates potential harm • How you retain logfile information. You need to make sure your data retention policies and logfiles include how long you'll retain this data

APPROACH	POINTS TO CONSIDER
Active/Pro-active technology monitoring services (These specialist services provide technology-based monitoring systems that actively monitor use across devices, through things such as keywords)	Use this approach where your risk assessment(s) suggests **high risk**. **Active monitoring** Where the system generates alerts for you to act on. This is effective where: • You have enough capability and capacity to interrogate and interpret the volumes of information and alerts generated by the system • You can assign appropriate safeguarding expertise to review, prioritise and take action on alerts **Pro-active monitoring** Where a third-party provider manages or supports alerts and may offer support with intervention. This is effective where you have a high number of devices operating. This system means: • Your safeguarding staff are actively and immediately alerted to genuine risk threats to health or life • You have a specialist organisation to provide additional capability and capacity to support your safeguarding staff Make sure you know whether your provider uses automation and what their team's safeguarding capability is.

Filtering and Monitoring Provider

QUESTION	WHAT TO LOOK OUT FOR	NOTES
Does your filtering and monitoring system adhere to the technical requirements? (get your checklist of the requirements here)	The provider needs to be compliant and adhere to best practice.	Yes
Does the provider work in, and align with, the education sector?	Some providers may not work with schools normally, so they may be unable to offer suitable support.	Yes

QUESTION	WHAT TO LOOK OUT FOR	NOTES
Is the provider based in the UK?	If you're looking at an international provider, be aware that their system may be geared more towards safeguarding issues that are less prominent in the UK. E.g. if you've selected a US provider, it may have a focus on school shooting content and may not adhere to requirements under the Prevent duty.	Yes
Can the provider give you school/education-specific case studies?	You want to see that the provider understands how to support schools and has a track record of doing this well.	Yes on the website
Can the provider give you a couple of school success stories with its system? What has been the impact of its product?	The provider should be able to explain how often they pick up a safeguarding alert or give an example of how their system helped to protect a child.	High uptake of schools using the system
Will the filtering and monitoring system work across all your devices?	Remember that the system needs to work on everything your school uses, from iPads to Chromebooks.	Yes
What technique does the provider use to filter websites?	This is to check how the provider categorises content and what the filter will see (you need to know how granular the filter is to decide if it's right for your school - will the filter only pick up domains or will it also pick up search terms?)	DNS Filtering. We also use Securly aware which picks up typed words
Does the provider offer granular or flexible filtering?	Some content you'll want to block for some year groups, but not others. Check to see if the provider gives you this option. This can help you to tackle 'over-blocking'. If you're in a multi-academy trust (MAT): make sure any sites you unblock are only unblocked for that specific school, and aren't automatically unblocked for all schools within the MAT	NA

QUESTION	WHAT TO LOOK OUT FOR	NOTES
Does the filtering and monitoring system identify individual users?	You need the provider to be able to flag which users have been searching for specific content so you can intervene (a general IP address alone is not helpful).	Yes
How will the provider monitor and how will it alert your school to concerns?	Some providers will triage any problems first before alerting your school to cases of genuine concern, while others will ping an alert to you whenever a pupil searches for something deemed as concerning. Bear in mind: • What capacity your school has to deal with alerts that come in. All alerts need to be taken seriously by the DSL, so be sure they have the time they need • That alerts need to be looked at by someone with safeguarding training and experience (for example, a child searching for 'Mia' may look like a pupil searching for a friend's name, when in reality this is an acronym for pro-bulimia content)	Emails sent to Executive Headteacher and Head of School

Blocked sites log

WEBSITE NAME AND URL	WHY IT'S BLOCKED	DATE BLOCKED	DATE UNBLOCKED (IF APPLICABLE)

Staff request form template to unblock a specific website(s)

Staff name and class:	
Website title and URL/link:	
Class you want the website unblocked for (if applicable):	
Reason why you want the website unblocked E.g. children need to access it for classwork, homework, revision	
Can we re-block this site after a specific date?	
Date the website can be re-blocked	

Sources

- Filtering and monitoring standards for schools and colleges - the Department for Education (DfE)
- Establishing appropriate levels of filtering - the UK Safer Internet Centre
- Appropriate monitoring: guide for education settings and filtering providers - the UK Safer Internet Centre
- Luke Godfrey is UK marketing director at Smoothwall, part of Qoria. Luke has a wealth of experience in the tech sector and has a real passion for protecting students online, enabling them to thrive in their digital lives
- Gareth Harle is an IT director who has worked managing and developing IT systems in education for almost 15 years across primary, secondary and FE sectors. His current role involves strategic planning and IT management across a multi-academy trust in Yorkshire
- Sian Stockham is deputy headteacher at King Ecgbert School in Sheffield. As an experienced senior leader, she has been involved in the leadership of safeguarding, online safety and IT strategy for well over a decade, and is passionate about the development of digital literacy and resilience in young people
- Kat Howard is a leading expert in digital safeguarding and wellbeing with over 20 years' experience working in and with schools. Kat supports schools with developing comprehensive strategies, implementing policies and procedures, conducting training, and establishing committees to promote student safety. Kat's unwavering passion for digital safeguarding and wellbeing drives her to provide expert advice and support on a day-to-day basis
- Tom Newton is a VP of product management at Smoothwall, part of Qoria. Tom has 20 years' experience in making the internet a safer place and is an expert in web filtering technology. Tom is always happy to speak with school leaders about their IT and safeguarding strategies

Technical Requirements

REQUIREMENT	
FILTERING SYSTEM	
Is it a member of the Internet Watch Foundation (IWF)?	☐ yes
Is it signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?	☐ yes
Does it block access to illegal content including child sexual abuse material (CSAM)?	☐ yes
Are you satisfied that the system manages the following content: • Discrimination • Drugs/substance abuse • Extremism • Gambling • Malware/hacking • Pornography • Piracy and copyright theft • Self harm • Violence	☐ yes

Is the filtering system:
• Operational
• Up to date
• Applied to all:
  ○ Users, including guest accounts
  ○ School-owned devices
  ○ Devices using the school broadband connection
	☐ yes

REQUIREMENT	
FILTERING SYSTEM	
Does the filtering system: • Filter all internet feeds, including any backup connections (e.g. a VPN) • 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 It is: • Age and ability appropriate for the users, and suitable for educational settings	☐ yes
Does the filtering system allow you to 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 you clear on how long logfile information (internet history) is retained and how it's stored?	☐ yes,
Are you clear on how the system does not over block access so it doesn't lead to unreasonable restrictions?	☐ yes,

REQUIREMENT	
FILTERING SYSTEM	

Does the filtering system meet the following principles?
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm
  ○ Can you vary the filtering strength? E.g. for staff?
• Circumvention
  ○ Can you identify and manage technologies used to circumvent the system, e.g. virtual personal networks (VPNs), proxy services and domain name system (DNS) over Hypertext Transfer Protocol Secure (HTTPS)
• Control
  ○ Can you control the filter yourselves to permit or deny specific content?
  ○ Can you log any changes as part of an audit trail?
• Contextual content filters
  ○ In addition to URL or IP-based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include artificial intelligence (AI) generated content. For example, being able to contextually analyse text on a page and dynamically filter
• Filtering Policy
  ○ Does your provider detail its approach to filtering, as well as over blocking?
• Group/multi-site management
  ○ Can your system be deployed centrally, with a central policy and dashboard?
• Identification
  ○ Does the system allow you to identify users?
• Multiple language support
  ○ Does the system manage relevant languages?
• Network level
  ○ Is the filtering provided at 'network level', i.e. it doesn't reply on software on user devices while at school
	☐ yes

REQUIREMENT	
FILTERING SYSTEM	

• Remote devices
  ○ Can the system filter devices where staff and/or pupils are working remotely?
• Reporting
  ○ Can you report inappropriate content?
  ○ Does the system provide clear historical information on the websites users have accessed or tried to access?
• Safe Search
  ○ Does the system have the ability to enforce 'safe search'?
	☐ yes

If users access content via mobile or through apps: Get confirmation that your provider can provide filtering on mobile or app technologies. They should also apply a technical monitoring system to devices using mobile and app content to reduce the risk of harm.	☐ yes
If your filtering provision is procured with a broadband service: Make sure it meets the needs of your school or college	☐ yes

REQUIREMENT	Ü
MONITORING SYSTEM	
Are incidents urgently picked up, acted on and the outcomes recorded?	☐
Are all staff clear on: • How to deal with these incidents • Who should lead on any actions	☐
Is device monitoring managed? (this could be by your IT staff or a third-party provider) Whoever is manging device monitoring will need to: • Make sure monitoring systems are working as expected • Provide reports on pupil device activity • Receive safeguarding training including online safety • Record and report safeguarding concerns to the DSL	☐ Sitech Support Ltd could intervene if inappropriate searches continue with pupils or staff members. Particular search terms that keep appearing could be addressed.
Is your monitoring data received in a format that your staff can understand?	☐ yes
Are users identifiable to your school or college, so you can trace concerns to an individual, including guest accounts?	☐ yes

REQUIREMENT	Ü
MONITORING SYSTEM	

Does your monitoring system alert you to behaviours associated with:
• Content
  ○ Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
• Contact
  ○ Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
• Conduct
  ○ Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying
• Commerce
  ○ Risks such as online gambling, inappropriate advertising, phishing and/or financial scams
	☐ yes

REQUIREMENT	Ü
MONITORING SYSTEM	

Does the monitoring system meet the following principles:
• Age appropriate
  ○ Can you vary your strategy to take age, vulnerability, or specific situations (e.g. boarding schools) into account
• Audit trail
  ○ Are any changes to the strategy logged so no one can make changes on their own?
• Bring your own device (BYOD)
  ○ If your system can monitor staff and pupils' personal devices, make sure this is done according to your data management policies. For example, will your system monitor devices out of school hours?
• Data retention
  ○ Be clear on what data is stored, where and for how long (including any backup data)
• Devices
  ○ Make sure your system is clear about which devices it covers
• Flexibility
  ○ Make it clear how keywords can be added or removed
• Group/multi-site management
  ○ Can your strategy be deployed centrally, with a central policy and dashboard?
• Harmful image detection
  ○ To what extent is visual content monitored and analysed?
• Impact
  ○ How do monitoring results impact your policy and practice?
	☐ yes

REQUIREMENT	Ü
MONITORING SYSTEM	

• Monitoring policy
  ○ How do you tell all users that you're monitoring their online access?
  ○ How do you communicate your expectations on appropriate use to pupils and staff?
• Multiple language support
  ○ Can the system manage relevant languages to your school?
• Prioritisation
  ○ How are alerts prioritised?
  ○ What procedures do you have in place to allow staff to respond to alerts rapidly?
• Remote monitoring
  ○ Can the system monitor devices where staff and/or pupils are working remotely?
  ○ Are users aware of this? Are you clear if these devices are only monitored during school hours?
• Reporting
  ○ How are alerts recorded, communicated and escalated?
	☐ Yes
	Staff meeting for TAs and teachers

Do your staff: • Provide effective supervision • Take steps to maintain awareness of how devices are being used by pupils • Report any safeguarding concerns to the DSL	☐ yes
If users access content via mobile or through apps: Have you applied a technical monitoring system to these devices?	☐ yes Staff use apps and webpages that are all filtered