



Filtering and Monitoring Checklist Register

In line with the [DfE filtering and monitoring standards in schools and colleges](#), this checklist template has been developed as a basis to support schools and colleges in meeting the required standards. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

Last updated:	Date: 17.9.24	Name/Position: Katie Bennett / Lee Pearson
---------------	---------------	---

Roles and Responsibilities

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Carol Robertson
Senior Leadership Team Member	Responsible for ensuring these standards are met and: <ul style="list-style-type: none"> • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports <p>Ensure that all staff:</p> <ul style="list-style-type: none"> • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns 	Katie Bennett Acting Head Jill Stroud DSL Catherine Eccleston DSL Maxine Morris – Head of Schools ICT Chris Smith – Schools ICT Infrastructure Manager
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: <ul style="list-style-type: none"> • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems 	Katie Bennett Acting Head Jill Stroud DSL Catherine Eccleston DSL
IT Service Provider	Technical responsibility for: <ul style="list-style-type: none"> • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems 	Chris Smith – Schools ICT Infrastructure Manager Lee Pearson – Schools ICT Primary Team Manager

Reviewing your filtering and monitoring provision

Filtering System	
Filtering Provider and System	Smoothwall Filtering
Date Procured	May 2012
Date last reviewed	1 st April 2023

Monitoring System	
Monitoring Provider and System	Smoothwall Monitor
Date Procured	May 2012
Date last reviewed	1 st April 2023

Review Team [should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor]	Chris Smith – Schools ICT Infrastructure Manager Lee Pearson – Schools ICT Primary Team Manager
Review Date	September 2025
Previous Review Date	September 2024
Link to last review	

Review Checklist	
the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)	N
what your filtering system currently blocks or allows and why	Y
any outside safeguarding influences, such as county lines	Y
any relevant safeguarding reports	Y
the digital resilience of your pupils	Work in progress
teaching requirements, for example, your RHSE and PSHE curriculum	Y
the specific use of your chosen technologies, including Bring Your Own Device (BYOD)	Y
what related safeguarding or technology policies you have in place	Y
what checks are currently taking place and how resulting actions are handled	Y

all staff know how to report and record concerns	Y
filtering and monitoring systems work on new devices and services before release to staff / pupils	Y
blocklists are reviewed and they can be modified in line with changes to safeguarding risks	Y

Recommendations / Mitigating Actions

Use of iPads and other tablet devices will not identify an actual user of the device as there isn't a login to the device. The report will contain the IP Address of the device which IT can correspond to device. Schools need to have processes in place for recording which device was used by which user for these to be cross-referenced against reports. At Sherdley all devices have been numbered and offset against class registers. This reduces the number of children who may be using the device. A timetable ensures this can be further reduced to 2 possible children.

Data Protection Impact Assessment

Schools and colleges that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third-party providers

Link to DPIA	
Conducted by	
Date conducted	

Regular Reports

Type of Report	Filtering / Monitoring
Producer of report	Chris Smith – Schools ICT Infrastructure Manager
Recipient of report	Headteacher
Frequency of report	Weekly, immediate notifications of incidents regarding adult content and self-harm

Monitoring data is received in a format that your staff can understand	
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	

System Checks

Filtering System				
Date checked	31/08/2023			
Checks conducted by	Lee Pearson - Schools ICT Primary Team Manager			
Device	Location	Logged in as	Check Conducted	Result
SPC-PUP-LIB-D08	School Library	Spc-pupil-test	888.com	Blocked

Confirm your filtering provider is:	
<ul style="list-style-type: none"> a member of Internet Watch Foundation (IWF) 	Y
<ul style="list-style-type: none"> signed up to Counter Terrorism Internet Referral Unit list (CTIRU) 	Y
<ul style="list-style-type: none"> blocking access to illegal content including Child Sexual Abuse Material (CSAM) 	Y

Monitoring System				
Date checked	As above filtering system			
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result
