ONLINE SAFETY

Make the annual filtering and monitoring review useful

A practical review structure for governors, SLT, DSLs and IT - focused on how controls work across the school's real users, devices and services.

DSLs	SLT	Governors	IT leads

HOW TO USE THIS BRIEFING

Use this briefing to plan, challenge or record the annual review and the technical checks that support it.

DECISION SNAPSHOT

If you only read one page

Start with the decision, then use the rest of the briefing to test evidence and plan implementation.

THE CORE DECISION

The annual review should not be a supplier certificate. It should show that roles are clear, the school's risk profile is understood, controls have been tested and resulting actions are owned.

Why this matters now

Annual assurance

DfE says filtering and monitoring provision should be reviewed at least once every academic year, with governors and proprietors holding strategic responsibility.

Changing technology

Cloud apps, off-site devices, encrypted traffic and AI-generated content can create routes that older test approaches do not cover.

Safeguarding plus IT

Effective review needs safeguarding context from the DSL and technical evidence from IT, supported by SLT and governors.

What good looks like

- Named SLT, governor, DSL and IT responsibilities
- A review shaped by age, SEND, EAL, locations and local risks
- Tests across pupil, staff, guest and administrator contexts
- Coverage of school devices, BYOD, off-site use and new services
- An alert-review and escalation process understood by staff
- A recorded action plan, not just a pass or fail statement

A sensible first action

- Agree the review owner and participants before testing begins.
- Create a test matrix covering users, devices, networks and locations.
- Review serious incidents, exceptions and known safeguarding themes.
- Record every check, finding, action, owner and review date.

CURRENT GUIDANCE NOTE

Publication timing: KCSIE 2025 remains in force until 31 August 2026. KCSIE 2026 takes effect on 1 September 2026. Always use the version currently in force.

SCHOOL REALITY

Where sensible plans often become difficult

These are common implementation problems in schools. They are not signs of failure; they are reasons to make dependencies, evidence and ownership visible.

Coverage is fragmented

A network filter may not govern mobile data, home use, unmanaged devices, some apps or content generated inside an AI service.

Blocking is not monitoring

Blocking reduces access; monitoring identifies concerning behaviour or content for review. Both need purpose, ownership and proportionate operation.

Context matters

A technically correct alert still needs safeguarding judgement, while a technical exception may create a wider online-safety risk.

Change happens between reviews

New devices, apps, SSIDs, user groups and supplier changes can alter protection after the annual review is signed.

Warning signs to investigate

- The review is completed only by the supplier or only by IT
- Tests cover one device, one user type or one school location
- Mobile data, off-site use, BYOD and new apps are not considered
- No one can explain who checks alerts and what happens next
- Exceptions and temporary allow rules are not reviewed
- Findings are recorded without owners or completion dates

LEADERSHIP PRINCIPLE

Ask for enough technical detail to support a decision, but keep the outcome expressed in school terms: learning, safeguarding, continuity, workload, cost and accountability.

DECISION FRAMEWORK

Questions that turn reassurance into evidence

Use the third column to agree what the school should be able to see, retain and review. Evidence should be current, understandable and linked to an owner.

DECISION AREA	LEADERSHIP QUESTION	EVIDENCE TO REQUEST
Governance	Who has strategic, safeguarding, technical and oversight responsibility?	Named roles, terms of reference and reporting route
Risk profile	What risks are specific to age, SEND, EAL, local context and recent incidents?	Online-safety risk assessment and incident themes
Scope	Which users, devices, networks, sites, remote routes and cloud services must be covered?	Coverage map and explicit exclusions
Filtering	What is blocked or allowed for each user group, and why?	Policy mapping, category settings and exception register
Monitoring	Which activity creates an alert and who reviews it?	Alert workflow, review frequency, escalation and sample records
Testing	Have checks covered the school's realistic user, device and location combinations?	Dated test matrix, results, screenshots and actions
AI content	Can the solution address real-time, personalised or AI-generated content where required?	Supplier capability statement and school risk decision
Change control	How are new devices and services checked before release?	Technical acceptance checklist and change records

How to use the table

Do not expect every item to be perfect before acting. Record the current position, the risk or service impact, the agreed action, the owner and a realistic target date. Review high-impact gaps first.

IMPLEMENTATION ROUTE

Move in controlled, visible stages

The sequence matters: establish the current position, prove the important controls or user journeys, then embed review into normal school governance.

PREPARE **Define context and scope**	• Assign SLT, governor, DSL and IT roles • Review incidents, risks, exceptions and technology changes • Create the users-devices-locations-services test matrix
REVIEW AND TEST **Gather evidence**	• Test filtering and monitoring from safeguarding and technical perspectives • Confirm alert response, staff reporting and escalation • Record limitations, workarounds and supplier dependencies
ASSURE AND IMPROVE **Close the loop**	• Agree actions, owners, risk decisions and target dates • Report a clear summary to governors or proprietors • Schedule risk-based checks between annual reviews

Measures leaders can follow

01
Full test-matrix coverage

02
Alert ownership confirmed

03
Exceptions reviewed

04
Actions closed by target date

KEEP THE PLAN REALISTIC

Align major changes to exams, census, payroll, admissions, safeguarding reviews and the limited windows available for disruptive work. Build support and rollback into the plan, not after it.

LEADERSHIP CHECKLIST

What to confirm before closing the review

A completed checklist is useful only when exceptions, evidence and actions are recorded. Use it as a review prompt rather than a compliance certificate.

☐ Strategic and operational roles are assigned	☐ Filtering categories match policy and curriculum need
☐ The school's risk profile informs the review	☐ Monitoring alerts have a clear review process
☐ Pupil, staff, guest and admin groups are tested	☐ AI-generated and dynamic content is considered
☐ Owned, shared and unmanaged devices are considered	☐ New services are checked before deployment
☐ Every site and relevant network route is included	☐ Tests, findings and exceptions are logged
☐ Off-site use and mobile-data limitations are recorded	☐ Governors receive assurance and an action plan

Minimum evidence pack

01
Role statement

02
Risk profile

03
Coverage map

04
Test log

05
Exception register

06
Governor assurance summary

Decision record

Record what was reviewed, who contributed, the evidence considered, any limitations, the decision made, actions and owners, and the next review date. This gives future leaders and suppliers a clear starting point.

ABOUT OPSWISE

School-focused support, security and planning

OpsWise helps schools make technology decisions in context - joining technical delivery with safeguarding, data protection, budget, supplier and operational needs.

How OpsWise can help

- Independent annual review facilitation
- Technical testing across users and devices
- DSL, SLT and governor evidence pack
- Remediation and ongoing control checks

What an initial discussion covers

- What is happening now
- Which outcome matters most
- What evidence is already available
- A proportionate next step, even if that is not a managed service

A PRACTICAL NEXT STEP

Turn the questions into a clear school IT plan.

OpsWise can help the DSL and IT lead run a practical review, document the evidence and turn findings into clear actions without replacing the school's safeguarding judgement.

hello@opswise.co.uk | 0203 907 6865

www.opswise.co.uk
86-90 Paul Street, London EC2A 4NE

Authoritative sources

DfE: Filtering and monitoring core standard

DfE: Keeping children safe in education

DfE: Generative AI product safety standards

Guidance checked 19 August 2026. Always consult the latest authoritative version. This briefing provides general information and a decision framework; it is not legal advice, certification or a guarantee of compliance or outcomes.