



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Filtering and Monitoring Standard and Assurance Checklist

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Contents

1. Purpose and scope.....	3
2. Statutory and regulatory framework	3
3. Definitions	4
4. A risk-based and documented approach	4
5. Filtering requirements.....	5
6. The challenge of different device types	6
7. Primary and secondary: proportionate monitoring	7
8. Artificial intelligence	7
9. Monitoring, reporting and the human element.....	8
10. Data logging and records.....	9
11. Data protection.....	9
12. Incident response and review	9
13. Annual review (KCSIE 2026).....	10
14. Training and awareness	10
Appendix A - Online safety risk assessment (template).....	11
Appendix B - Annual review and system functionality log (template)	12
Appendix C - Potential questions to ask your IT provider/team	13
Appendix D - Quick Guides	15

1. Purpose and scope

This policy sets out how the school provides a safe online environment through appropriate filtering and monitoring, and how it manages the online safety risks that arise from a wide range of devices and technologies, including artificial intelligence (AI).

It complements, and should be read alongside, the Department for Education's Filtering and monitoring standards for schools and colleges, the wider DfE digital and technology standards, and the statutory guidance Keeping Children Safe in Education (KCSIE). Where school owned or managed technology is used away from the school site, this policy applies to that use as well.

Scope

- Any device that connects to the school's network and uses it to access the internet.
- Any school-owned or school-managed device that accesses the internet through third-party connections, such as home or public Wi-Fi.
- All users - pupils, staff, governors, contractors, volunteers and visitors.
- Cloud services, apps and generative AI tools accessed through or on school systems or accounts.

2. Statutory and regulatory framework

This policy is grounded in the following statutory and recommended sources:

- **Keeping Children Safe in Education 2026** - statutory safeguarding guidance, in force from 1 September 2026. It requires the effectiveness of filtering and monitoring to be reviewed at least once every academic year, led by a named SLT member with support from the DSL and IT, and recorded.
- **DfE Filtering and monitoring: core standard** - one of the six core digital and technology standards, updated in 2026 to bring generative AI and AI-generated content explicitly within scope of filtering and monitoring.
- **DfE digital and technology standards** - including the cyber security, broadband and digital leadership and governance core standards that schools should meet by 2030.
- **DfE Generative AI in education guidance and product safety expectations** - referenced by KCSIE 2026 to help schools assess and manage AI-related risk.
- **UK GDPR and the Data Protection Act 2018** - monitoring logs contain personal data, so a Data Protection Impact Assessment (DPIA) is required.

3. Definitions

Filtering

Filtering is a preventative measure. It identifies and blocks access to illegal, inappropriate and potentially harmful content in formats including text, images, audio, video and, following the 2026 update to the DfE standard, AI-generated content. Filtering should also be able to identify words used in search terms and in AI prompts and block on the basis of key words.

Monitoring

Monitoring is a reactive measure. It observes what users are doing on devices and, in some cases, records that activity. Monitoring can be manual - for example, a teacher viewing screens as they move around a classroom - or technical, using software that generates reports or alerts. Monitoring does not block; it enables staff to notice and respond.

Reporting

Reporting is the process by which filtering and monitoring systems produce reports or alerts that can be reviewed and acted on. Reports should identify the user, device, time, activity and category of concern where possible. Safeguarding concerns must be triaged and/or shared promptly with the DSL or DDSL, recorded where action is taken, and used to review controls, supervision and education. The concerns generated by reporting platforms, where supported, can be imported automatically into safeguarding platforms making tracking of concerns easier and linking them to other indicators of risk.

Artificial intelligence (AI)

For this policy, AI includes generative AI tools that create text, images, audio or video, AI chatbots and companions, and features embedded within other apps and services. AI is treated as an extension of online safety, not as a separate discipline.

4. A risk-based and documented approach

Filtering and monitoring decisions are based on the age, stage and needs of pupils and on an assessment of risk, not on a single fixed configuration. This reflects the DfE principle that filtering should block harmful content without unreasonably restricting teaching and learning, and the KCSIE caution against over-blocking.

The school will:

1. Maintain a documented risk assessment for online safety, covering content, contact, conduct and commerce risks, and AI-enabled harms such as deepfakes, nudification apps and unsafe chatbots.
2. Record which filtering categories (and specific sites) are blocked or allowed, for which user groups, and the reasons why. The categories will depend on the filtering tool used.
3. Document all requests to unblock or block sites, who approved them, and when they were reviewed. Requests to block must be acted on immediately.
4. Review and document the risk assessment and configuration at least annually, and after any significant incident or change.
5. Schools who issue managed devices to pupils may deem it appropriate to block all access between set hours to support a healthy approach to technology use and sleep.

5. Filtering requirements

Solution requirements

Any filtering solution used by the school must be provided by a supplier that is:

- a member of the Internet Watch Foundation (IWF);
- signed up to the Counter-Terrorism Internet Referral Unit (CTIRU) list; and
- blocking access to illegal content, including child sexual abuse material (CSAM).

The school will obtain documentary evidence that the solution meets these criteria.

Coverage and defaults

- School-owned devices are filtered both on and off the school site.
- Any device connecting to school systems should be filtered, irrespective of ownership, including cloud resources.
- No device or user on a school-managed network may reach the internet unfiltered, including via backup or failover connections.
- The default position is to block internet access where filtering is not available.
- Although school owned devices are monitored by software whether on or off the school network, reports will only be reviewed during the school day and when the school is open.
- Where children use school devices outside of the school day, their use of the internet is the responsibility of their parent/guardian. The school may intervene if inappropriate use occurs outside of school.
- In residential settings filtering may be relaxed at certain times of the day to provide

a solution which more closely resembles access in a home. Those responsible for residential settings should receive appropriate reports during specified hours to reflect their extended roles.

Configuration by role

Filtering for staff should generally match filtering for pupils, so that websites staff use in lessons are also accessible to pupils. Exceptions - for example, staff access to social media for a legitimate purpose - must be approved by SLT, documented and reviewed annually. Guests, visitors and unauthenticated users receive the most restrictive profile.

6. The challenge of different device types

A single network-level filter is no longer sufficient. Learning now happens across managed and personal devices, on and off site, and increasingly inside apps and AI tools. The table below summarises the main device types, the challenge each presents, and the expected control.

Device type	Key filtering / monitoring challenge	Expected control
School-managed desktops and laptops (on network)	Baseline case; risk of unfiltered failover or backup connections.	Full filtering and monitoring; block internet by default if filtering is unavailable, including on backup links.
School-owned devices used off-site	Home and public Wi-Fi bypass the network-level filter.	Device-level (endpoint) filtering and monitoring that travels with the device.
Tablets and shared devices (primary)	Shared accounts make activity hard to attribute; young users.	Restrictive profile, adult supervision, and identifiable users so concerns trace to an individual.
School-managed iPads	iPads restrict the ability to monitor what is typed into, or displayed in apps	Use of specific browsers which can be monitored. Restricting access to specific browser for searching or AI use
Mobile phones / BYOD	Personal devices and mobile data can avoid school controls entirely.	Clear mobile phone policy (KCSIE 2026), guest network with most restrictive filtering, and MDM where devices are enrolled.

		Provide token based access to WiFi
SEND / assistive-technology devices	Eye-gaze, switch access and communication aids may struggle with standard controls.	Risk-assessed, accessible controls that maintain safeguarding without blocking legitimate access.
Guest / visitor / unauthenticated devices	Unknown risk profile and no accountable user.	Apply the most restrictive filtering profile, equivalent to the youngest pupils. Provide token based access to WiFi
Cloud and app-based access (incl. AI apps)	Activity happens inside apps and generative AI tools, not just web pages.	Solution able to inspect or report on in-app and AI activity; high-risk AI tools risk-assessed and controlled.

7. Primary and secondary: proportionate monitoring

Monitoring should be proportionate to the age and independence of learners. In practice this creates a spectrum, with the emphasis shifting from adult supervision in the early years towards technical measures as pupils gain more independent and individual device access.

Primary phase (and younger / SEND learners)

- Strong emphasis on active adult supervision - devices used in shared, sightline-visible spaces.
- Higher default filtering restrictions; a smaller, curated set of approved sites and apps.
- Monitoring is often achieved through the classroom adults directly viewing screens and walking the room.
- Age-appropriate online safety education built into the curriculum.

8. Artificial intelligence

KCSIE 2026 confirms that AI sits within safeguarding, online safety, filtering and monitoring, staff training and governance. AI-generated content - including deepfakes and AI-generated nude or semi-nude images - is treated as carrying the same safeguarding weight as other material, and the online safety “4Cs” now explicitly include generative AI applications

under contact risk.

The school will:

1. Assess the risks from AI-generated content, deepfakes, nudification apps and AI chatbots as part of its online safety risk assessment.
2. Ensure filtering and monitoring can inspect or report on AI activity where it occurs within apps, and can act on AI prompts and search terms.
3. Consider whether a solution able to handle real-time, dynamic, personalised and AI-generated content is required, as prompted by the 2026 DfE standard.
4. Risk-assess high-risk AI tools and control or block access where appropriate, informed by the DfE generative AI product safety expectations.
5. Ensure AI-related incidents are recognised, recorded, escalated and referred through the same safeguarding routes as other concerns.

9. Monitoring, reporting and the human element

KCSIE is clear that filtering and monitoring are not a substitute for professional judgement. Technology supports people; it does not replace them. The right people, working together and using their expertise, make the system effective.

Monitoring and Reporting requirements - pupils

- Monitoring is managed by school IT staff who receive appropriate safeguarding and online safety training.
- Reports and alerts about activity that may pose a safeguarding risk follow a documented route and go to the safeguarding team, never to a single person.
- Data is provided in a format staff can understand, and users are identifiable so concerns can be traced to an individual, including on shared or guest accounts.
- It should be possible for DSLs to create monitoring reports for high risk children where required

Monitoring and Reporting requirements - staff

- Different monitoring of categories should be used for staff. Safeguarding risks should still be monitored as for pupils. Categories around bullying or self harm should be reviewed to prevent invasion of privacy.

Why the human element matters

- Manual monitoring - staff viewing and supervising screens - remains a core method, especially in primary settings.
- Staff professional curiosity is essential: recognising manipulated images, unusual behaviour, or AI-assisted harm that a filter will not flag.
- A strong, whole-school safeguarding culture, led by the DSL with IT as a delivery partner, is what turns alerts into timely, child-centred action.
- No single professional holds the full picture, so information sharing between staff, the DSL and IT is vital.

10. Data logging and records

Filtering and monitoring systems must allow the school to identify:

- device name or ID, IP address, and the username of the individual using the device;
- the time and date of the activity;
- where appropriate, the search term or AI prompt used;
- the content or webpage accessed or blocked; and
- the category of the content, as defined by the solution.

The school / IT provider will keep a system functionality log recording when checks took place, who carried them out, what was tested and any resulting actions. Checks will cover a range of school-owned devices (including off-site), geographical areas across the site, user groups, and new devices before release. The school / IT provider may use the SWGfL testing tool to confirm blocking of illegal CSAM and unlawful terrorist content.

11. Data protection

A DPIA must be completed for every filtering and monitoring solution before it is procured and used, because log files are likely to contain personal data linked to usernames. The DPIA is reviewed when the solution or its use changes. Records are retained in line with the school's retention schedule and the monitoring strategy is integrated with the school's data protection policy and any data sharing agreements.

12. Incident response and review

Following a reportable incident, the DSL and IT lead will review the effectiveness of the filtering and monitoring solution and identify:

- lessons learnt;

- improvements that can be implemented;
- limitations and how these can be mitigated; and
- whether the solution remains fit for purpose.

Findings are shared with SLT and the responsible governor, and with the local authority where appropriate.

13. Annual review (KCSIE 2026)

The effectiveness of filtering and monitoring is formally reviewed at least once every academic year. The review is led by the named SLT member responsible for filtering and monitoring, with support from the DSL and IT, and the governing body is accountable for the outcome.

Each review will:

- Confirm what works well and where the solution is limited or poses unacceptable risk.
- Test across device types, user groups and locations, including off-site and AI activity.
- Check the configuration and roles have not changed or been deactivated.
- Produce documented evidence that the review took place and record the actions arising.

14. Training and awareness

- All staff receive online safety training as part of safeguarding induction and updates, now including AI-enabled risks.
- The SLT filtering and monitoring lead receives training to carry out an informed annual review, including an understanding of the DfE standards.
- Staff who monitor systems receive role-specific safeguarding training.
- It should be clearly communicated to all staff what is captured by the monitoring tools and if staff devices are filtered and monitored when not on school networks.
- Pupils receive age-appropriate online safety education, and parents and carers are informed of relevant policies.

Appendix A - Online safety risk assessment

Completed by:

Date Completed:

Date for review:

Risk / scenario	Likelihood	Impact	Control / mitigation and owner
Access to harmful or illegal content	[H/M/L]	[H/M/L]	- Filtering & Monitoring systems in place - Children supervised when using technology - Age appropriate online safety education built in to the curriculum
Pupil use of a nudification or deepfake AI app	[H/M/L]	[H/M/L]	- Filtering & Monitoring systems in place - Children supervised when using technology - Age appropriate online safety education built in to the curriculum
Off-site device bypassing filtering	[H/M/L]	[H/M/L]	- Devices only issued to staff members - Staff aware of the expectations and read and sign an ICT agreement
Over-blocking restricting teaching	[H/M/L]	[H/M/L]	- Sites blocked on the recommendation of Schools ICT - Blocks can be removed if deemed appropriate by DSL/DDSL.
Shared account preventing attribution	[H/M/L]	[H/M/L]	- Pupils and staff issued with individual logins - Technology numbered and children issued with the same number each time.

Appendix B - Annual review and system functionality log

Use to evidence the KCSIE 2026 annual review and routine functionality checks.

Date	Led by (SLT lead)	What was tested / checked	Findings and actions
<i>[Date]</i>	<i>[Name / role]</i>	<i>[Devices, sites, user groups, AI tools]</i>	<i>[Findings and follow-up]</i>
<i>[Date]</i>	<i>[Name / role]</i>	<i>[Devices, sites, user groups, AI tools]</i>	<i>[Findings and follow-up]</i>

Appendix C - Potential questions to ask your IT provider/team

Use these questions when reviewing current provision, preparing for the annual filtering and monitoring review, or commissioning a new or revised filtering and monitoring solution. The aim is to obtain clear evidence, not reassurance alone.

Coverage and scope

- Which users, devices, networks and locations are covered by filtering and monitoring?
- Are school-owned devices filtered and monitored when used off site, including on home or public Wi-Fi?
- What happens if the filtering service, internet connection or backup connection fails?
- How are guest, visitor, BYOD and unauthenticated devices controlled?

Filtering configuration

- Can you provide the current filtering categories, allowed sites and blocked sites for each user group?
- How do you ensure illegal content, including CSAM and terrorist content, is blocked?
- Is the provider a member of the Internet Watch Foundation and signed up to the CTIRU list?
- How are requests to block or unblock content recorded, implemented and reviewed?

Monitoring, alerts and reporting

- What activity is monitored, and what is not monitored, on each device type?
- Which alerts go to safeguarding staff, who receives them, and how quickly are they delivered?
- Can reports identify the user, device, date, time, search term or AI prompt, site or app, and category of concern?
- Can the DSL create or request targeted reports for higher-risk pupils where this is justified?
- How are false positives, false negatives and repeated low-level alerts reviewed?

AI, apps and emerging risks

- Can the solution identify or report on AI prompts, AI-generated content and activity

Filtering and Monitoring Standard and Assurance Checklist

within apps?

- How are high-risk AI tools, chatbots, image generators, deepfake tools and nudification apps identified and controlled?
- How quickly can new sites, apps or categories of concern be added to the filtering or monitoring configuration?

Evidence, testing and review

- What evidence can you provide that the current system meets the DfE filtering and monitoring standard?
- When was the last functionality check completed, what was tested, and what actions resulted?
- How will you support the school's annual review of filtering and monitoring?
- Can you provide a written summary of known limitations, residual risks and recommended improvements?
- What changes would require the school to update its DPIA, risk assessment, policy or user notices?

Appendix D - Quick Guides

Staff summary - what all staff need to know

Filtering and monitoring help keep pupils safe online, but they do not replace staff judgement, supervision or safeguarding procedures. All staff should understand the following points.

- **Filtering** helps stop users accessing illegal, inappropriate or harmful content.
- **Monitoring** helps the school notice concerning activity so that staff can respond.
- Staff must report any online safety or safeguarding concern to the DSL or safeguarding team, even if a system has not generated an alert.
- If a site is blocked incorrectly, staff should follow the school's agreed block or unblock request process rather than bypassing controls.
- If harmful content appears on a screen, staff should prioritise pupil safety, preserve relevant information where safe to do so, and report the concern promptly.
- IT manages the technical controls, but safeguarding decisions sit with the DSL and senior leaders.

Role-based quick guide

If you are...	You need to...	Speak to...
Teacher	Supervise device use, follow the policy, and report concerns or inappropriate access.	DSL / DDSL
Teaching assistant or support staff	Alert the teacher, DSL or DDSL if online activity, behaviour or content causes concern.	Teacher / DSL
DSL or DDSL	Review alerts, record safeguarding action, and advise on risk, context and escalation.	SLT / IT support
IT support	Maintain controls, provide evidence, support reports and explain technical limitations clearly.	SLT lead / DSL
Governor	Seek assurance that the school has effective controls, trained staff, clear records and an annual review.	Headteacher / SLT lead

What to do if...

If...	Staff should...
Harmful or inappropriate content appears	Keep pupils safe, avoid unnecessary exposure, preserve relevant information where safe, and report to the DSL or DDSL.
A pupil bypasses filtering or uses a personal device inappropriately	Follow the behaviour and safeguarding procedures, report the concern, and do not rely on technical controls alone.
AI is used in a concerning way	Treat it as an online safety or safeguarding concern. This includes deepfakes, harmful prompts, unsafe chatbots and AI-generated images.
A legitimate learning resource is blocked	Use the agreed request process. Do not use personal accounts, mobile data or workarounds to bypass filtering.
You receive or are shown a monitoring alert	Share it promptly with the DSL or DDSL, unless you are already responsible for triaging that alert.
You are unsure	Ask the DSL or DDSL. It is better to report a concern that later needs no action than to miss a risk.