

Important Changes Filtering and Monitoring

The Department for Education (DfE) has published [Keeping Children Safe in Education \(KCSIE\) 2026](#), the statutory safeguarding guidance that all schools and colleges in England must follow from 1st September 2026. While many of the changes build on existing expectations, this year's update contains several significant developments for online safety including additions around filtering and monitoring, artificial intelligence, and safeguarding accountability

Filtering and Monitoring Reviews Become an Annual Requirement

One of the most important changes in KCSIE 2026 is that schools and colleges must now ensure that the effectiveness of their filtering and monitoring systems is reviewed "at least once every academic year." Previously, annual review was encouraged through the DfE Filtering and Monitoring Standards, but the timing was not stated as explicitly within KCSIE itself.

The guidance now makes it clear that governing bodies and proprietors should ensure:

- Appropriate filtering and monitoring systems are in place.
- Their effectiveness is reviewed at least once every academic year.
- Schools can demonstrate that these reviews have taken place.

There Must Be Clear Accountability

KCSIE 2026 introduces a stronger emphasis on named responsibility for filtering and monitoring reviews. The guidance states that reviews should be carried out by:

"the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support."

This is a notable shift as responsibility can no longer sit solely with a technical team, or external service provider. Instead, schools are expected to demonstrate leadership oversight, supported by safeguarding and technical expertise.

For many schools, this will require reviewing governance arrangements and ensuring responsibilities are formally assigned and understood.

Record-Keeping on Filtering Is Now a Requirement

Another significant addition is the requirement to keep records of filtering checks. KCSIE 2026 states that reviews should include checks that filtering works appropriately

across all internet-connected devices in all relevant locations, and that a record should be kept of these checks.

With the condition of keeping a record schools should now consider evidencing:

- When checks were conducted.
- Which devices and environments were tested.
- Identified issues.
- Actions taken to address concerns.

Generative AI Enters Filtering and Monitoring Expectations

Artificial intelligence continues to feature more prominently throughout safeguarding guidance, and KCSIE 2026 directly connects AI with filtering and monitoring responsibilities.

The guidance references the DfE publication "[Generative AI: product safety expectations](#)", explaining that it supports schools in understanding how filtering and monitoring requirements apply to generative AI within educational settings.

This reflects the reality that schools are increasingly deploying AI-powered tools while simultaneously managing emerging risks including, inappropriate AI-generated content, unsupervised interactions with AI systems and data protection concerns.

Filtering and Monitoring Now Feature More Prominently in DSL Responsibilities

KCSIE 2026 makes filtering and monitoring expectations more visible throughout the guidance. The role of the Designated Safeguarding Lead (DSL) must explicitly include understanding filtering and monitoring systems and processes, and this responsibility should be reflected in the job description.

Likewise, staff safeguarding training must include an understanding of filtering and monitoring expectations, relevant roles and responsibilities and how concerns should be escalated. While many schools already addressed these areas, KCSIE 2026 makes the expectation far more explicit.

The 4Cs Framework is Updated

The well-established 4Cs model remains central to online safety guidance, but KCSIE 2026 modernises the framework to reflect today's digital landscape.

Within the guidance:

- Contact risk now explicitly includes harmful interactions involving generative AI applications that simulate human interaction, such as AI chatbots and companion-style systems.

- Conduct risk explicitly references making, sending or receiving explicit images, including images generated using AI.

This is an important acknowledgement that safeguarding risks increasingly arise not just from interactions with people online, but now also from interactions with AI-powered technologies.

"Nudes and Semi-Nudes" Becomes the Consistent Terminology

A particularly notable change concerns the language used around nude imagery. KCSIE 2026 adopts the term "nudes and semi-nudes" throughout the guidance when referring to the creation, sending or sharing of nude or semi-nude images by young people under 18. This includes imagery that is:

- Self-generated.
- Created by another individual.
- Digitally altered.
- Entirely AI-generated.
- Described as "deepfakes" or "deep nudes".

The revised wording replaces broader terminology used in the consultation draft, helping align safeguarding language with existing UKCIS guidance and terminology already familiar to many schools.

Importantly, KCSIE explains that the term "nudes" is used because it is "the most widely understood by young people" and best reflects the range of behaviours being addressed.

The guidance also explicitly references consensual and non-consensual making or sharing of nudes and semi-nudes, including those generated using AI.

Cybersecurity Recognised as a Safeguarding Issue

Another welcome development is the stronger connection between cybersecurity and safeguarding. KCSIE 2026 introduces a direct reference to the Cybersecurity standards for schools and colleges and positions cyber resilience within wider safeguarding responsibilities. The guidance states that schools should protect personal information and ensure appropriate cyber security systems are in place as part of safeguarding children.

This reflects an increasingly important reality: compromised safeguarding records, stolen pupil data, and cyber incidents can all have direct safeguarding consequences.

Preparing for September

The new KCSIE 2026 updates continue the inclusion of new and emerging online safety focusses from a predominantly technical concern to a leadership-led safeguarding responsibility.

The strengthened requirements around annual review, documented checks, named accountability, AI safety, cyber security and DSL oversight show a clear expectation that schools must take a more proactive and evidenced approach to safeguarding children online.

For schools, now is the time to review filtering and monitoring arrangements, confirm ownership of responsibilities, and ensure that AI, cyber security and emerging online risks are fully reflected within safeguarding frameworks ahead of the guidance coming into force on 1 September 2026.