KCSIE 2026

What it expects, and where we help

ContentKeeper and StudentKeeper
A practical mapping for schools and colleges

Supporting online safety in England

Based on the final September 2026 guidance
October 2026



The mapping

This guide maps the online-safety expectations in Keeping children safe in education (KCSIE) 2026 against what ContentKeeper and StudentKeeper do, and what stays with your school.

Governing bodies and proprietors should ensure appropriate filtering and monitoring are in place, with effectiveness reviewed at least once every academic year. An SLT member leads the review, supported by the DSL and IT staff, with checks across internet-connected devices in relevant locations and a record of those checks.
Paragraph 173, summarised

No supplier can make a school KCSIE compliant. Ativion helps you manage access, identify potential concerns and gather evidence, so your staff can make informed decisions and act on what matters.

Filtering and monitoring

KCSIE paragraphs 173–177. SLT: senior leadership team. DSL: designated safeguarding lead.

What KCSIE expects	How Ativion helps	What your school owns
Appropriate filtering Blocking harmful content without overblocking	ContentKeeper provides more than 90 content categories, IWF and CTIRU blocklists that users cannot override, safe search and restricted YouTube settings. SSL inspection provides visibility into encrypted web traffic.	Set and review what is blocked for whom. Check that policies and required blocklists are enforced in your deployment.
Appropriate monitoring Context beyond the website visited	StudentKeeper provides supported on-screen visibility, safeguarding keyword detection, alerts to designated staff and contextual evidence for investigation. Optical character recognition (OCR) helps identify concerning text.	Review alerts, set thresholds and act on concerns. Staff assess context and decide the safeguarding response.
Different access for different users	Policies can be applied by user type, year group, teaching group and time of day, with directory mapping so access follows identified users.	Set policies that match your risk assessment. Check group membership and approved exceptions.
Coverage across devices and locations	ContentKeeper combines inline filtering on the school network with cloud protection for supported managed devices beyond school. Network filtering covers personal and guest devices using that connection. Controls help tackle unauthorised VPNs and proxy circumvention.	Confirm coverage, including unmanaged devices and alternative connections. Off-site protection depends on supported, healthy clients. No filtering system prevents every bypass attempt.

Filtering and monitoring in daily practice

KCSIE paragraphs 163 and 173–177, supported by the DfE filtering and monitoring core standard.

What KCSIE expects	How Ativion helps	What your school owns
An annual effectiveness review With a record of checks and actions	Reporting by user, device and time, blocked and attempted access, policy configuration, alert history and change histories help you examine effectiveness. CPOMS integration can support the transfer of concerns into safeguarding records.	Name the SLT lead, carry out the review, record findings and actions, and report through your governance arrangements. Product evidence informs the review; it does not complete it.
Blocking without unreasonable restriction	Group exceptions and granular video settings help preserve educational access. Dynamic Safe-Listing allows embedded YouTube and Vimeo videos from trusted learning platforms. Controls can restrict Shorts and comments without blocking an entire platform.	Balance protection with teaching and access to support. Give staff a route to challenge a block, and approve and review exceptions.
Filtering outside teaching hours Lettings and community use	Inline filtering applies to devices using the protected school connection, including personal and guest devices outside teaching hours.	Set suitable policies for community users, evenings and holidays. Agree monitoring and response arrangements when usual staff are absent.
Consistent practice across a trust	Parent and child organisation structures support central policies across sites. Role-based access can give schools access to their own data while supporting trust-level oversight.	Agree what is set centrally and what schools can vary. Keep each school's risk assessment, review and safeguarding responsibilities clear.

Make the evidence useful

Record when checks took place, who carried them out, what was tested and the action taken. Include relevant devices, locations and connections, and revisit coverage when your technology or pupils' needs change.

Agree who receives monitoring reports and who responds. The DfE standard calls for at least weekly incident reporting and immediate reporting of high-risk concerns. Your reporting arrangements, staffing and escalation procedures need to work together to achieve this.

Change histories help you understand changes to the system. Your school's own records should also capture concerns, decisions, reasons, actions and outcomes.

Online safety and the four areas of risk

KCSIE paragraphs 164–169. Filtering and monitoring contribute in different ways; both sit within your wider safeguarding approach.

What KCSIE expects	How Ativion helps	What your school owns
Content Harmful or illegal material	ContentKeeper restricts access through category policies and relevant blocklists. StudentKeeper adds context from concerning text and visible activity, including within permitted services. Some harms are addressed within related categories rather than under an identical label.	Set proportionate restrictions and provide preventative education. Preserve access to legitimate information and support.
Contact Harmful interactions, including with AI applications	Filtering governs which services are reachable. Monitoring can highlight relevant text and visible activity within supported capture settings.	Respond to disclosures and patterns. Monitoring does not reveal every message or conversation.
Conduct Bullying and harmful image sharing	Filtering can restrict harmful destinations, while monitoring can identify concerning activity on permitted platforms. Chrome-based image blurring can help reduce exposure to explicit images.	Teach safe behaviour, provide reporting routes and follow safeguarding procedures, including the relevant Part Five processes.
Commerce Gambling, scams and phishing	Category and threat controls help reduce exposure to commercial risks.	Provide financial and online-safety education and maintain wider security and incident-response arrangements.

Two harms worth looking at in detail

What KCSIE expects	How Ativion helps	What your school owns
Self-harm, suicide and eating disorders	Monitoring includes relevant safeguarding keyword categories, helping staff identify concerning language with contextual evidence. Filtering settings can also contribute, while keeping legitimate health and support resources available.	Decide who receives alerts, how quickly they are reviewed and how pupils are supported.
Misogyny and violence against women and girls	Related filtering categories can restrict harmful material. Monitoring keywords can help identify language associated with misogyny and gender-based violence.	Provide preventative education and act on concerning behaviour, including behaviour dismissed as banter.

Generative AI and safeguarding leadership

AI risks form part of the online-safety framework in KCSIE paragraphs 165–169.

What KCSIE expects	How Ativion helps	What your school owns
Understanding AI use	The AI Services category covers general-purpose AI tools. Other AI-enabled services may sit in a content category, such as adult content, and appear in reporting there.	Decide which tools are suitable and approved. Consider reports across relevant categories rather than treating AI Services as a complete inventory of AI use.
Seeing beyond the website visited	StudentKeeper can capture visible prompts and responses within supported screen capture and OCR activity, providing context beyond a URL.	Assess what the context means for a particular pupil. This is not continuous inspection of every AI conversation.
Governing access on your terms	Allow or block the AI Services category, permit named tools and apply access policies by group or time.	Set and teach your AI policy. Assess tools for safeguarding, privacy, age suitability and educational purpose.

Roles training and policy

What KCSIE expects	How Ativion helps	What your school owns
DSL understanding Paragraphs 127–129 and Annex B	Role-based dashboards, documentation and product training help safeguarding staff understand the systems and their information.	Provide a senior DSL with the authority, knowledge, resources and cover to lead safeguarding, supported by IT expertise.
Staff training Paragraphs 12 and 153–154	Ativion can train your team on its systems. This supports, but does not replace, whole-school safeguarding training.	Provide induction and regularly updated training, with safeguarding updates as required and at least annually.
Phone-free default Paragraph 170	Filtering supports access policies where devices use the protected school connection.	Set and enforce the phone policy and manage exceptions. Network filtering does not control personal mobile-data connections.

Understand the coverage in your own school

KCSIE asks you to judge systems against your school's risks. That means understanding both what the technology provides and how it is deployed.

Filtering and monitoring have different roles

ContentKeeper assesses URLs and web traffic to apply access decisions. This is different from continuously assessing content generated inside an allowed page, such as a chatbot response. StudentKeeper can add screen-level evidence within its supported capture scope; staff still need to review that evidence and decide what it means.

Device and language coverage

ContentKeeper clients extend filtering beyond school on Windows, macOS, ChromeOS and iOS. Android clients are not supported. Off-site filtering depends on the client being installed and healthy. Personal and guest devices receive network filtering while using the protected school connection.

Filtering coverage and monitoring coverage are not interchangeable. Personal devices are not monitored by default; monitoring requires a supported client and an appropriate bring-your-own-device policy. Check the coverage of apps, browsers and connections in your actual deployment.

Supplied monitoring keyword lists are predominantly English; other languages require custom lists. Assess these needs separately from website categorisation. Where DNS-level filtering is used, it works at domain level and does not inspect page content.

Privacy and proportionality

Explain monitoring arrangements to users, assess their privacy impact and give staff access appropriate to their responsibilities. Agree how captured information is stored, retained and used in safeguarding decisions.

Talk it through against your own setup

Every school's devices and risk profile are different. Our team can walk through this mapping with your DSL and IT lead, discuss coverage and show how product information can support your annual review.

Explore ContentKeeper and speak to our team

Official guidance

Keeping children safe in education 2026

DfE filtering and monitoring core standard

Ativion, October 2026. Based on the final September 2026 guidance for England, in force from 1 September 2026. This guide maps relevant online-safety responsibilities, not every KCSIE requirement, and should be read alongside the full guidance. Functionality and coverage depend on deployment and configuration.

Additional Guidance

The external links included in this article are provided for your convenience and further reading. Ativion does not control or endorse the content of third-party websites and accepts no responsibility for their content, accuracy, or availability.

Why language matters: The NSPCC explains why changes in safeguarding terminology are important. **LINK**

Regulated activity: Guidance on the expanded definition of regulated activity and its implications for DBS checks **LINK**

Appropriate terminology: Learn how the *No Such Thing* campaign helped establish accepted terminology for reporting Child Sexual Abuse Material (CSAM). **LINK**

Filtering and Monitoring: Explore the latest 2026 updates, including strengthened expectations for AI, user-generated content, mobile devices, and apps. **LINK**

DBS process review: Read about the review of the Disclosure and Barring Service process and its implications for safer recruitment and vetting. **LINK**

DBS Strategic Plan 2026–2027: View the Disclosure and Barring Service's strategic priorities for the 2026–2027 business year. **LINK**