Appropriate Monitoring for Schools

May 2025

Monitoring Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”. Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to [Content, Contact, Conduct, Contract] risks from the school’s or college’s IT system*” however, schools will need to “*be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*.”

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined ‘appropriate monitoring’ standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is ‘appropriate’ for them.

Company / Organisation	NetSupport Limited
Address	NetSupport House, Market Deeping, Peterborough, PE6 8NE
Contact details	01778 382270 / support@netsupportsoftware.com
Monitoring System	classroom.cloud by NetSupport – cloud-based safeguarding, IT management and classroom instruction
Date of assessment	1 October 2025

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟨

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
- Are IWF members	🟩	NetSupport has been a member of the IWF since January 2016. The IWF keyword list is integrated into our own safeguarding keyword library.
- Utilisation of IWF URL list for the attempted access of known child abuse images	🟨	Not currently utilised.
- Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟨	While NetSupport has worked with the CTIRU since autumn 2016 and its police-assessed list of unlawful terrorist content (URL blacklist) is integrated into our NetSupport DNA 'on-prem' monitoring software, it is not currently deployed with classroom.cloud.
- Confirm that monitoring for illegal content cannot be disabled by anyone (including any system administrator) at the school	🟨	To give our customers maximum flexibility in how they use our software, we do give schools the option to disable monitoring in the classroom.cloud Administrator's cloud-based web portal if required, but the main system admin can avoid inadvertent enabling/disabling of the software by colleagues by applying appropriate permissions to each user role.

Illegal Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.	🟩	Integrated grooming/child abuse (IWF keywords) keyword libraries are in our monitoring software. This means we can monitor all content typed, copied or seen within any application that would suggest a young person is vulnerable to exploitation in these areas. Phrase matches are graded by level of risk using our

		🟩	contextual intelligence-based risk indexing tool. Our lists are supplemented and kept current by our team’s own ongoing research and in partnership with relevant charities and local community organisations.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.	🟩	Integrated grooming/child abuse (IWF keywords) keyword libraries in our monitoring software. This means we can monitor all content typed, copied or seen within any application that would suggest a young person is vulnerable to exploitation in these areas. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. Our lists are supplemented and kept current by our team’s own ongoing research and in partnership with relevant charities and local community organisations.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.	🟩	Integrated safeguarding keyword libraries in our monitoring software mean we can detect text typed, copied or seen within any application that would indicate exposure to or promotion of extreme sexual violence. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. For schools using our enhanced safeguarding package, the image analyser can also identify adult imagery of this nature, alerting safeguarding staff where such content is displayed.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.	🟩	Combined with our extensive keyword library, we have our image analyser tool available for schools that have our enhanced safeguarding package which monitors and detects inappropriate images displayed on students’ screens from websites, apps and media. As with the keyword monitoring,

		🟩	results that appear trigger an alert which is then flagged to staff who are set to receive alerts about these triggers.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.	🟩	We have gambling and financial/fraud keyword libraries in our monitoring software. This means we can monitor all content typed, copied or seen within any application that would suggest a young person is vulnerable to exploitation in these areas. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. Our lists are supplemented and kept current by our team's own ongoing research and in partnership with relevant charities and local community organisations.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.	🟩	Integrated safeguarding keyword libraries in our monitoring software include terms linked to racism, discrimination and religious intolerance. The system monitors all text typed, copied or seen within any application that could indicate the use or promotion of racially or religiously aggravated language or behaviour. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. For schools using our enhanced safeguarding package, the image analyser can also detect racist imagery to support early identification and intervention.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.	🟩	Integrated safeguarding keyword libraries in our monitoring software include terms linked to violence, aggression and extremist behaviour. The system monitors all text typed, copied or seen within any application that would suggest intent to promote or glorify violent acts. Phrase matches are graded by level of risk using our contextual

		🟩	intelligence-based risk indexing tool. For schools using the enhanced safeguarding package, the image analyser can also detect weapon imagery to support early intervention.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.	🟩	There is no dedicated keyword category for illegal immigration or people smuggling. However, classroom.cloud's existing safeguarding libraries, such as grooming, sexual exploitation and radicalisation, include related terms that highlight indicators of trafficking or exploitation. The system monitors all text typed, copied or seen within any application. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.	🟩	Separate suicide and wellbeing keyword libraries monitor all text typed, copied or seen within any application that indicates a young person is considering suicide or being exposed to material encouraging or facilitating suicide. Our ongoing research and work with specialist partners and charitable organisations ensure these libraries remain current. Keywords in this category are automatically assigned high-priority status to raise the profile of alerts to safeguarding staff.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.	🟩	Integrated safeguarding keyword libraries in our monitoring software include terms related to the non-consensual sharing of intimate or sexual images. The system monitors all text typed, copied or seen within any application that indicates image sharing, coercion or exploitation. For schools using the enhanced safeguarding package, the image analyser can also identify adult imagery of this nature, alerting

		🟩	safeguarding staff where such content is displayed.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.	🟩	Drugs and weapons keyword libraries in our monitoring software detect text typed, copied or seen within any application that relates to the sale, purchase or promotion of illegal substances or weapons. Slang and alternative terminology are included to capture emerging trends. For schools using the enhanced safeguarding package, the image analyser can also detect drug or weapon imagery to support early identification and intervention.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.	🟩	Integrated grooming and sexual exploitation keyword libraries in our monitoring software detect text typed, copied or seen within any application that indicates coercion, manipulation or exploitation for sexual purposes. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. For schools using the enhanced safeguarding package, the image analyser can also identify adult imagery of this nature to support safeguarding teams.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.	🟩	The radicalisation keyword library in our monitoring software detects text typed, copied or seen within any application that indicates exposure to, or promotion of, terrorist or extremist material. While classroom.cloud does not directly integrate the CTIRU police-assessed list of unlawful terrorist content, its safeguarding libraries are aligned with Prevent guidance and are kept current through ongoing research and collaboration with relevant safeguarding and community partners. Phrase matches are graded by level of risk using our

		🟩	contextual intelligence-based risk indexing tool. For schools using the enhanced safeguarding package, the image analyser can also identify radicalisation-related imagery to support timely safeguarding intervention.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling	🟩	The gambling keyword library in our monitoring software detects text typed, copied or seen within any application that relates to gambling, betting or online gaming for financial gain. It includes terminology linked to addiction and betting apps to help identify vulnerable users. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.	🟩	classroom.cloud includes safeguarding keyword libraries designed to identify harmful content, including language linked to bullying, harassment, hate speech, violent or abusive behaviour, and the encouragement of dangerous behaviour. The system monitors text typed, copied or seen across supported applications and browsers, helping schools identify potential risks to wellbeing. Phrase matches are logged within the safeguarding portal and graded by contextual risk level using the system’s intelligence-based risk indexing tool, ensuring staff can prioritise concerns appropriately.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion,	🟩	Integrated safeguarding keyword libraries in our monitoring software include terms linked to hate speech, discrimination and

	sex, or sexual orientation. . Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010	🟩	intolerance. The system monitors all text typed, copied or seen within any application that expresses or promotes prejudice, hostility or violence towards protected groups. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. For schools using the enhanced safeguarding package, the image analyser can also detect racist imagery to support safeguarding teams.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses	🟨	classroom.cloud does not monitor for or detect malware, hacking activity, or the use of anonymous browsing or filter bypass tools. These areas sit outside the scope of its safeguarding monitoring functionality. The system's keyword libraries are focused on safeguarding categories such as adult content, radicalisation, racism, weapons and drugs. While schools can add custom keywords to address local concerns, classroom.cloud is not a cybersecurity or filtering product and does not analyse network or executable activity.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions	🟨	classroom.cloud does not analyse or fact-check online content for accuracy. It does not identify misinformation or disinformation in the sense of evaluating whether information is true or false. The system focuses on safeguarding indicators through keyword and phrase monitoring, including terms related to extremism or online manipulation including keywords related to harm, but it does not assess the factual reliability of material viewed or shared by users.
Pornography	displays sexual acts or explicit images	🟩	The adult keyword library in our monitoring software detects text typed, copied or seen within any

		🟩	application that relates to or promotes pornographic material. Acronyms, slang and abbreviations are included to ensure broad coverage and reduce false positives. For schools using the enhanced safeguarding package, the image analyser can also detect adult imagery, alerting safeguarding staff where such content is displayed.
Self Harm and eating disorders	encourages, promotes, or provides instructions for self harm or eating disorders	🟩	Separate self-harm and eating disorders keyword libraries in our monitoring software detect text typed, copied or seen within any application that indicates vulnerability, distress or engagement with self-harm or disordered eating behaviours. Our ongoing research and collaboration with specialist partners ensure these libraries remain current. Keywords in this category are automatically assigned high-priority status to raise the profile of alerts to safeguarding staff.
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.	🟩	Integrated safeguarding keyword libraries in our monitoring software include terms linked to violence, coercion, misogyny and harmful gender stereotypes. The system monitors all text typed, copied or seen within any application that promotes or normalises gender-based violence or abuse. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. For schools using the enhanced safeguarding package, the image analyser can also identify related imagery to support early safeguarding intervention.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects classroom.cloud’s safeguarding technology is designed to help schools meet their statutory safeguarding duties by monitoring content typed, copied or seen within applications, browsers and online communication platforms. The system’s keyword libraries, developed in collaboration with safeguarding specialists and community partners, are continually updated to reflect emerging risks, trends and slang across multiple languages. Schools can add their own custom terms to reflect local safeguarding priorities and opt to share them with NetSupport for wider inclusion in future updates.

For schools using the enhanced safeguarding package, the image analyser extends protection by identifying inappropriate or harmful imagery across the categories Adult, Drugs, Racism, Radicalisation and Weapon. Keyword and image alerts are graded by level of risk using the contextual intelligence-based risk indexing tool, ensuring that safeguarding teams can quickly identify and support vulnerable students.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access	🟩	With classroom.cloud, schools can create online safety groups and apply tailored safeguarding settings to each. This allows staff to configure which keyword categories and image analysis options are active, determine who receives alerts, and manage student visibility within the ‘Report a concern’ tool. These group-based settings ensure monitoring remains appropriate to the age and needs of different cohorts while supporting proportionate safeguarding oversight.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	Safeguarding administrators can configure which priority levels and keyword categories trigger alerts for each user role. Alerts rated Medium and above generate email notifications to nominated safeguarding staff. In the safeguarding portal, new alerts are flagged as “new” until reviewed; they can be annotated, forwarded, reassigned or dismissed. For

	🟩	schools using CPOMS or Tes MyConcern, triggered events and reported student concerns can be linked directly to the corresponding student in those systems via integration. Existing alert configurations can be adjusted or removed at any time through the admin interface.
• Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.	🟩	An Audit Log records actions, system changes and configuration updates made by all classroom.cloud users across each site. Events such as adding/removing users or devices, licence changes and deleting false-positive triggers are all captured. These audit entries cannot be disabled or removed and may be filtered, searched or exported to support accountability and oversight.
• BYOD (Bring Your Own Device) – if adopted by the school and the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location	🟩	classroom.cloud supports BYOD in two ways. Students can join classes on personal devices using a class code, enabling short-term participation without installing additional monitoring tools. Alternatively, schools can configure closer monitoring by registering personal devices through their tenancy and deploying the classroom.cloud student application. In this model, monitoring applies only when devices connect to the school network and is governed by the school's BYOD or Acceptable Use Policy, which includes parental consent. Privacy settings determine when safeguarding and classroom features are active, ensuring

	🟩	proportionate and transparent oversight.
● Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision	🟩	classroom.cloud retains safeguarding and audit log data on a rolling 13-month basis, automatically purging older records in line with data minimisation and UK GDPR requirements. Activity monitoring data is retained for 90 days. If a school's subscription ends or is terminated, all account data is deleted after a 30-day grace period. Schools can export data to maintain their own long-term safeguarding records where required under their statutory obligations.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	classroom.cloud requires the installation of a platform-specific student application or browser extension on each device to enable monitoring. The software supports Windows 10, 11, macOS (Catalina 10.15 or later), iOS 14 or later (iPad), Android 12 or later, and Chrome OS116 or later. Devices can be deployed individually or centrally using tools such as Group Policy or Intune. A 64-bit operating system is required for image analysis.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy	🟩	Schools can amend safeguarding keyword coverage in line with policy. Administrators can add custom keywords, adjust the priority of existing phrases, and enable or disable keyword libraries for specific groups or at site level. Changes take effect immediately and are recorded in the audit log for accountability. This ensures schools can respond quickly

	🟩	to emerging vocabulary or local risks across all supported languages.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	classroom.cloud provides a clear organisational hierarchy, allowing trusts and multi-site schools to manage all locations centrally. The Organisation Admin can create individual sites, apply global settings, and delegate site-level control where required. Default policies can cascade from the organisation to each site, while local administrators can override specific settings to reflect local needs. Safeguarding users assigned to multiple sites can view triggered events through a unified dashboard, and aggregated reporting provides central oversight across all schools within the organisation.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).	🟩	The Image Analysis feature in classroom.cloud scans visual content displayed on student screens (websites, applications, media) and flags material in the categories of Adult, Drugs, Racism, Radicalisation and Weapon. This feature is available only with Enhanced Safeguarding enabled and only on Windows devices with a 64-bit OS. Schools can enable or disable each category, set detection sensitivity (default ~95 %), and require phrase monitoring to be active. When an image match is triggered, a screenshot is taken (which can be obfuscated by default) and routed as a safeguarding alert.

- Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the application of appropriate configurations for individual users.	🟩	classroom.cloud attributes all safeguarding and classroom activity to identified users and devices. Students are recognised through their device name, logged-in username, or authenticated Microsoft 365 or Google Workspace account, and those joining via class code must identify themselves by name before connection. Each triggered event records the student, device, application, time and site to ensure traceability. On mobile devices, monitoring and configuration apply when the student is signed in and connected to the school tenancy, ensuring safeguards remain active across all supported platforms.
- Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	Users are made aware that their online access is being monitored through local school communication, supported by NetSupport's guidance for inclusion in Acceptable Use and privacy policies. The classroom.cloud Student app operates with a visible icon when active, and schools are encouraged to explain its safeguarding purpose to students, parents and staff. NetSupport provides Privacy by Design documentation, a Data Processing Agreement, and role-based guidance to help schools configure and communicate their monitoring approach transparently and lawfully.
- Mobile and app content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the monitoring system operate across mobile	🟩	classroom.cloud supports safeguarding across web and app environments on Windows, Chrome OS, macOS, iOS and Android.

devices and app content. Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this.	🟩	Keyword monitoring detects text typed, copied or seen within browsers, applications and communication platforms such as Microsoft Teams when the school’s tenancy is connected. On mobile devices, monitoring operates through the classroom.cloud Student app and is active only while students are signed in and connected to the school tenancy. Image analysis is currently available only on Windows 64-bit systems as part of the Enhanced Safeguarding package. The Android app does not currently include the “safeguarding” feature.
• Multiple language support – the ability for the system to manage relevant languages?	🟩	classroom.cloud supports safeguarding keyword libraries in more than 18 languages, including English, Arabic, Bengali, Czech, Danish, Dutch, Finnish, French, German, Greek, Hindi, Italian, Mandarin, Polish, Portuguese, Romanian, Spanish, Swedish, Turkish and Urdu. All supported languages use the same contextual intelligence-based risk indexing to ensure consistent grading of alerts. Schools can add their own custom keywords in any language, which can be shared with NetSupport for broader inclusion. The classroom.cloud interface and user dashboards also support multiple display languages for staff access.
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?	🟩	classroom.cloud applies a prioritisation framework to triggered events using severity levels and a contextual intelligence-

	🟩	based risk index. Each phrase or image match is assigned a priority (Low, Medium, High, Urgent) which determines whether the event is simply logged, captures a screenshot or video, or sends email alerts. The risk index evaluates contextual factors (such as time of day, previous alerts, applications used, device history) to highlight high-risk events and vulnerable students for expedited review by safeguarding staff.
• Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users. Monitoring should focus on school-owned and managed devices. When shared devices are used, schools must ensure users log in individually. This allows monitoring systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.	🟩	classroom.cloud supports both in-school and remote monitoring when configured by the school. Monitoring is linked to tenancy authentication rather than physical location, meaning that if a student remains logged in on a school device, safeguarding tools will remain active even off-site. Schools can prevent unintended monitoring (for example, when a device is used at home) by restricting operation to defined hours, networks or IP ranges within the privacy and safeguarding settings. Keyword and image monitoring, alerting and “Report a concern” operate identically for remote users while active. When monitoring is inactive, no safeguarding data is captured.
• Reporting – how alerts are recorded within the system?	🟩	Triggered events and alerts are recorded within the Online Safety portal, showing the student, device, site, application, time and contextual information. Safeguarding staff can filter, sort and export data by date, category or site to identify

	🟩	trends or repeated patterns of concern. Reports can be shared directly with CPOMS and Tes MyConcern, ensuring accurate transfer of safeguarding information. All reporting actions are logged in the audit trail and historical alerts remain accessible for 13 months in line with data retention policy.
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity	🟩	classroom.cloud integrates directly with CPOMS and Tes MyConcern to support effective safeguarding case management. Safeguarding staff can send triggered events, contextual information and screenshots securely from the Online Safety portal to their chosen case management system for further investigation and record keeping. Integration is configured by administrators within safeguarding settings and uses secure API connections in line with data protection and confidentiality requirements.

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

classroom.cloud does not provide a third-party proactive monitoring service or external review team. All safeguarding alerts are managed by the school's own designated staff through the Online Safety portal. The system uses automated contextual analysis to grade alerts by risk level and priority, helping schools focus attention where it is most needed. Schools receive guidance and training materials to support their internal safeguarding capability and ensure consistent, informed responses to triggered events.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

classroom.cloud actively supports schools in meeting their statutory duties under the latest *Keeping Children Safe in Education (KCSIE)* guidance through its safeguarding tools, training and wider professional development resources. The platform provides keyword and image monitoring aligned with KCSIE expectations for appropriate filtering and monitoring, supported by clear audit trails, reporting and data protection documentation. NetSupport also provides a suite of free resources and webinars, including a recent session led by CEO Al Kingsley MBE and Mark Anderson (Head of Education and ICT Evangelist) focused specifically on the latest KCSIE updates and their practical implications for schools. These materials help staff interpret statutory expectations, evidence compliance and strengthen whole-school safeguarding practice.

How does your monitoring system identify and respond to activity involving Generative AI technologies (e.g. AI prompts, content creation, or platform use)?

In your response, please explain how your system captures or analyses user interactions with Generative AI tools; to what extent logs or alerts reflect potential safeguarding risks associated with AI-generated content (such as harmful prompts or inappropriate use of image and text generation); any known limitations—whether technical, privacy-related, or device-specific—that may affect your system's ability to monitor such activity; and what guidance you provide to schools to support their understanding and management of Generative AI-related risks.

classroom.cloud monitors the use of generative AI platforms by capturing and analysing text typed, copied or seen within supported applications and browsers. This allows schools to identify interactions with AI tools such as ChatGPT, Copilot or Gemini, and to detect inappropriate or harmful prompts that may present safeguarding concerns. All captured events are logged within the Online Safety portal and graded by contextual risk, enabling staff to prioritise responses effectively.

The system does not analyse or interpret AI-generated content, assess bias or accuracy, or evaluate the intent of AI outputs. Monitoring applies only when devices are connected to the school tenancy, and the system cannot view encrypted or off-network traffic.

To support schools in managing emerging AI-related risks, NetSupport provides extensive professional development and guidance materials. These include R.I.S.E. Magazine articles exploring AI in education and online safety, the ListEd podcast, NetSupport Radio, and the Getting Started series, all of which help schools build understanding of ethical and responsible AI use. Recent webinars, including those hosted by NetSupport's CEO, Al Kingsley MBE, and Mark Anderson (Head of Education) have focused specifically on the latest KCSIE updates and practical approaches to AI literacy and safeguarding.

Together, these resources help schools meet DfE filtering and monitoring standards and KCSIE expectations by equipping leaders and staff to interpret AI-related activity confidently and maintain a proactive safeguarding approach.

Monitoring Provider Self-Certification Declaration

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Al Kingsley
Position	CEO
Date	25th November 2025
Signature	