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	Lightspeed Systems®
Address	Phoenix House, Christopher Martin Road, Basildon, Essex, SS14 3EZ
Contact details	+44 (0) 20 4534 5200 / sales@lightspeedsystems.com
Monitoring System	Lightspeed Filter™, Lightspeed Alert™
Date of assessment	June 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		Lightspeed Systems has been a member of IWF since 2009.
• Utilisation of IWF URL list for the attempted access of known child abuse images		Lightspeed Systems immediately updates our Filter categories to match the IWF hash list and completely lock down access.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Lightspeed Systems works with CTIRU to block the police assessed list of unlawful terrorist content.
• Confirm that monitoring for illegal content cannot be disabled by anyone (including any system administrator) at the school		All illegal content is automatically placed in "locked categories" which can't be disabled by any member of staff, regardless of admin access.

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.		Any online material depicting child sexual abuse will be placed in the *porn.illicit* category in Lightspeed Filter™ which is permanently blocked. The category is constantly updated using our advanced web crawlers and the latest IWF lists. Lightspeed MDM™ can prevent inappropriate apps from being installed on school-issued devices, and Lightspeed Alert™ can immediately notify admins of related terms being used.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.		Locked categories such as *offensive* would stop students being able to access websites that would encourage coercive behaviour. Our safeguarding solution, Lightspeed Alert, also notifies the school when students type anything related to violence or cyberbullying.

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.		This content will be blocked using our sealed *offensive* category, blocking all gratuitous images of sexual violence and our broader *violence* category.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.		All potentially illegal pornographic material is locked in the *porn.illicit,* containing potentially illegal and more severe pornographic material.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		S*ecurity.malware* contains a combination of the *Security.virus, Security.spyware* and *Security.phishing* categories to protect users' personal information and block all scams. Any users attempting to reach these categories can be easily found and exported in Lightspeed Filter's reports.
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.		*The* permanently locked *violence.hate* and *offensive* categories would protect students from content that encourages racism or xenophobia of any kind.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.		Our *violence* category contains all sites that promote the use of physical force intended to harm or kill. Lightspeed Alert also notifies admins when students type anything related to violence.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.		Our *society.crime* category will automatically block anything related to crime and the justice system, including content promoting illegal immigration.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.		To prevent any students from looking at websites that promote or display self-harm schools and several different categories can be controlled such as *forums* and *adult.* Our safeguarding solution Lightspeed Alert uses advanced AI and a 24/7 safety specialist team to notify administrators instantly when a student types anything relating to self-harm online. Alert works across all productivity and education apps, files, chat including Microsoft

			Teams and Google Workspace and provides schools with a timeline of the event including screenshots and activity logs.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		The *porn.illicit* category blocks any intimate images shared on any site with Lightspeed Filter. The image scanning technology built into Lightspeed Alert identifies any sexual images and videos and users sharing or accessing them for intervention.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.		We have specific categories for blocking access to *drugs* and our *security.proxy* category prohibits applications such as Tor browser, blocking access to the Dark Web and illegal marketplaces.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		Filter's *porn.illicit* category would block all opportunity for sexual exploitation.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		Our *violence.extremism* category contains all the latest URLs from the Home Office that promote terrorism, terrorist ideologies, violence or intolerance—as well as URLs added by the worldwide education community.

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		Lightspeed Filter's gambling category blocks and reports on all websites related to gambling, casinos, betting, lottery and sweepstakes.
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.		Using Lightspeed Filter, schools can enable safe social media use with "read-only mode" and customisable on social media sites, block comments on YouTube with easy SmartPlay™ controls, and control app permissions using Lightspeed MDM to deter cyberbullying.

			Lightspeed Alert will detect instances of bullying and cyberbullying in real time, allowing schools to intervene before situations escalate. Trained in-house safety specialists will also conduct thorough reviews to assess context and severity, ensuring appropriate responses.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation. . Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010		Our *violence.hate* category contains sites that promote hostility against different groups. By leveraging AI-driven categorisation, we ensure that harmful material promoting unjust treatment is effectively restricted, fostering a safe and inclusive online environment for all students. This proactive approach not only protects students from exposure to discriminatory content but also supports educational institutions in upholding their legal obligations under the Equality Act, promoting equality and respect within the digital learning space.
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		Malware and other malicious content is blocked before it reaches the network. Our database categorises sites with demonstrated or potential security risks into several security categories, and for extra safety, all unknown URLs can be blocked.
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		In addition to the education-focused and continuously updated categories integrated into Lightspeed Filter, schools have the flexibility to customise their own policies by including local or targeted websites, platforms, and individuals known for disseminating disinformation.
Pornography	displays sexual acts or explicit images		Naturally, all pornographic material in the main *porn* category is blocked. In addition there are several other porn related categories for different

			languages and the *suspicious.script* category blocks javascript content frequently used for innapropriate sites such as pornography.
Self Harm and eating disorders	encourages, promotes, or provides instructions for self harm or eating disorders		Lightspeed Filter allows the utilisation of blocked-search key words related to self-harm and eating disorders. The *offensive* category blocks images that encourage self-mutilation and Lightspeed Alert proactively reports on any self-harm instances providing screenshots and a timeline of the events.
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		The *violence.hate* category blocks all URLs that would encourage harm against women. All social media sites are blocked by default to discourage misogynistic content and algorithms.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Lightspeed Systems utilises a sophisticated categorisation system, driven by both AI and a vast content database, to effectively classify websites and online content for educational purposes. This system categorises content into over 100 categories, which are continuously updated to reflect the latest online trends and threats. These categories help schools implement appropriate web filtering policies, ensuring a safe digital learning environment. Lightspeed's safeguarding and monitoring solutions are driven by AI web crawlers, an extensive content database, and third party integrations to ensure our URLs and categories are as up to date as possible.

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		Lightspeed Filter and Lightspeed Alert have been designed specifically for schools and colleges. It can be fully customised to perfectly match your organisational structure--tailoring policies for entire year groups down to individual users.

• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Assigned admins can receive alerts when students type words on the customisable flagged terms list. Schools can toggle on/off safety alerts for all or specific students with Lightspeed Alert. For product alerts, schools can subscribe to status.lightspeedsystems.com to receive alerts for product uptime, scheduled maintenance and ongoing issues.
• 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.		We have a full audit log of any changes made to any of our systems.
• 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		DNS-based filtering can be applied. In this way, traffic that should be blocked is given a false DNS response that directs the end user to an on-premise virtual appliance to apply filter policy decisions. These are based on user authentication or Filter group inheritance.
• 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		Lightspeed Systems is fully GDPR compliant and has access to student data only as requested by the school and only for the purposes of performing services on the school's behalf. We may collect personally identifiable information directly from children, including first name, last name, email address, password, IP address, year group, and school. Following termination or deactivation of a school account, Lightspeed Systems may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes, but all student data associated with

		the school will be deleted promptly.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		In the Lightspeed Community site, available to all customers and Partners, the devices and OS supported and the functions of each supported device for each OS are outlined in detail.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		Tiered administration across our products allows different levels of control to be permitted to different schools and users. Designated staff can add and edit keyword lists and create local allow and block lists. YouTube access can be managed by category, channel, and video. Teachers can control the internet in their individual classes using Web Zones to expand or constrict access with oversight.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Lightspeed Filter can be setup to have multiple schools, groups and users all managed and monitored from one centralised login. You can see a dashboard view of useful reports or use the reports tab to see a list of all the education-focused reports built in. You can also apply different levels of admin rights, access to reports and policies to members of staff in each school.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).		We filter based on where the image is hosted but also utilise image scanning for explicit imagery on the Google integrations for Lightspeed Alert. Lightspeed Filter allows schools to enforce Google safe search which blocks any harmful images students try to access.
• Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the		Lightspeed's Smart Agents will identify users and devices transparently, for non-agent

application of appropriate configurations for individual users.		devices we can prompt a captive portal or integrate with radius.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		While school acceptable/responsible use policies normally inform users that their online access is monitored, blocked access pages and internet lockouts for multiple attempts to access inappropriate content also communicate that access is being monitored.
• 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 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.		We can monitor all mobile and app content provided the delivery method itself allows external filtering and monitoring.
• Multiple language support – the ability for the system to manage relevant languages?		Our *world* categories contain websites from multiple countries that can be filtered accordingly. Flagged keywords can be added in any language to flag suspicious or concerning user activity. Further, we can enforce Google safe search, which has Google's own rules in multiple languages.
• 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?		Individual staff members can be designated to receive email alerts immediately when Flagged words are used in searches. A user will be locked out for repeated, persistent attempts to access blocked content.
• 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		Lightspeed's patented Smart Agents sit on every device ensuring that students are monitored at the same level when working remotely. Our After School Rules give administrators the option to relax restrictions at specific times and our Parent Portal

systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.		allows parents to see their children's online activity when working remotely and set basic restrictions on internet usage.
• Reporting – how alerts are recorded within the system?		Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group. Filter admins can also create custom reports and view live reports of web activity.
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity		We integrate directly with CPOMS to push high risk cases directly to their CPOMS tray for additional context and coverage outside of our own AI and in-house safeguarding and monitoring with Lightspeed Alert.

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.

AI-Powered Monitoring System
Lightspeed Alert offers robust proactive monitoring through its advanced AI technology, which continuously scans school devices for concerning online behaviours such as cyberbullying, self-harm, and explicit content in real-time. This system integrates seamlessly with Google and Microsoft platforms, ensuring comprehensive coverage across all devices.

Automated Detection and Alerts
The monitoring system utilises automation to provide:

- Real-time alerts for high-risk incidents, enabling early intervention
- Customisable alert settings tailored to specific school or user needs

Professional Safeguarding Support
Lightspeed Alert enhances its safeguarding capabilities with:

- A dedicated team of safety specialists who review alerts for context and threat level
- 24/7 support to ensure immediate response to potential dangers

Comprehensive Coverage
The system meets and exceeds the requirements outlined in the Keeping Children Safe in Education (KCSiE) guidelines, providing continuous surveillance and detailed reporting to support timely interventions.

Implementation and Training Support
Lightspeed offers extensive onboarding assistance, including deployment support and training resources, ensuring schools can effectively utilise the platform to protect students.
This proactive approach combines cutting-edge technology with human expertise, creating a secure online environment that prioritises student safety.

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

1. Enhanced Training and Staff Development

- **Comprehensive Training Modules**: Schools should develop training specifically aligned with KCSiE requirements to ensure that all staff, especially Designated Safeguarding Leads (DSLs), are well-informed about their safeguarding responsibilities.
- **Regular Updates**: Implementing ongoing training updates will help staff stay current with evolving safeguarding practices and legal obligations.

2. Improved Integration Capabilities

- **Seamless System Integration**: Strengthening the integration between existing safeguarding tools, such as Lightspeed Alert and CPOMS, can create a more cohesive safeguarding management system.
- **Customizable Solutions**: Schools should have access to customizable APIs that allow them to tailor their safeguarding solutions to meet specific needs.

3. Enhanced Monitoring and Reporting Features

- **Advanced Analytics**: Expanding dashboard capabilities to include detailed analytics can help schools identify trends and potential safeguarding issues more effectively.
- **Sophisticated Alert Mechanisms**: Implementing advanced alert systems for potential safeguarding concerns will enable quicker responses to incidents.

4. Strengthened Parent Engagement

- **Parent Portal Enhancements**: Expanding the capabilities of parent portals to provide insights into online activity can foster better communication between schools and families regarding online safety.
- **Resource Development**: Creating guides and resources for parents can help them support their children's online safety at home.

5. Technology Risk Management

- **Emerging Threat Detection**: Enhancing systems to identify and respond to new online threats will help schools stay ahead of potential risks.
- **Robust Filtering Controls**: Developing advanced filtering capabilities for educational content, particularly on platforms like YouTube, will ensure that students have access to appropriate resources while minimizing exposure to harmful material.

These enhancements will significantly bolster schools' ability to meet their KCSiE obligations, ensuring a safer environment for students and staff alike.

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.

Lightspeed Systems provides robust tools and frameworks to monitor, analyse, and respond to activity involving Generative AI technologies, such as AI prompts, content creation, and platform use. These tools are designed to ensure safe and ethical use of AI in educational environments while addressing safeguarding risks associated with AI-generated content.

Input Monitoring and Alerts

Lightspeed Systems can monitor and alert on any input into Generative AI platforms, such as ChatGPT or DALL-E, across most devices except iOS. This capability ensures that user interactions with Generative AI tools are captured and analysed for potential risks. The system generates real-time alerts for concerning activity, enabling swift intervention by school staff or administrators.

Advanced Filtering and Content Analysis

Lightspeed Filter, a core component of the system, provides comprehensive content filtering. It ensures that inappropriate or harmful content generated by AI tools is blocked or flagged. This includes:

- Filtering AI-generated text or images that may contain violent, sexual, or self-harm-related content.
- Blocking access to Generative AI platforms that are deemed inappropriate for educational use.

Policy Development

- Lightspeed assists schools in developing policies for the responsible use of Generative AI, including guidelines for acceptable use and consequences for misuse.
- Schools are advised to implement clear rules around AI-generated content, such as prohibiting its use for academic dishonesty or harmful purposes.

Customisable Controls

- The platform offers customizable controls to manage access to Generative AI tools. Schools can restrict or allow access based on grade level, subject, or individual student needs.
- Flexible guardrails, such as the AI Notify Tool, help teachers manage AI usage in classrooms while maintaining a safe learning environment.

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	Brian Thomas
Position	President and CEO
Date	1st June 2025
Signature