Appropriate Filtering for Education settings

May 2025

Filtering 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 filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Lightspeed Systems
Address	Phoenix House, Christopher Martin Road, Basildon, Essex, SS14 3EZ
Contact details	+44 (0) 20 4534 5200 / sales@lightspeedsystems.com
Filtering System	Lightspeed Filter™
Date of assessment	May 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.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Lightspeed Systems has been a member of IWF since 2009.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update		Web pages or URLs that depict indecent images of children, advertisements for such content, or links to it are illegal and constantly tracked by IWF (Internet Watch Foundation). Lightspeed Systems immediately updates its Filter categories to match the IWF list and completely lock down access.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		To assist schools in complying with the Prevent Duty Guidance of the United Kingdom Counter Terrorism and Security Act 2015, Lightspeed Systems has established the *violence.extremism* category. This category is populated with a list of web addresses that promote extremism and/or radicalisation and is provided from The Home Office in the UK. The *violence.extremism* category is updated each time the Home Office supplies us with a list. Advanced reporting features allow IT administrators to easily view Internet activity across the whole school- or drill down to individual user activity. Also, email alerts can be set up so suspicious search activity notifies designated staff.
• Confirm that filters for illegal content cannot be disabled by anyone at the school (including any system administrator).		All websites categorised as illegal in Lightspeed's extensive, constantly updated URL database are placed in sealed categories that cannot be allowed by any IT admin or member of staff in a school or organisation.

Describing how, their system 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 which is permanently blocked. The category is constantly updated using our advanced web crawlers and the latest IWF lists.
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™, built into the filter 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* category, 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.
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		Our *society.crime* category will automatically block anything related to crime and the justice

	offering illegal transportation or documentation.		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 an reports on any user who is attempting to access them. The image scanning technology built into Lightspeed Alert immediately identifies any sexual images, videos and users sharing 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 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

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling		Lightspeed Filter's gambling category blocks all websites related to gambling, casinos, betting, lottery and sweepstakes.
Hate speech / Discriminiatio n	Content that expresses hate or encourages violence towards a person or group based on something such as disability, race, religion, sex, or sexual orientation. Promotes the unjust or prejudicial treatment of people with protected characteristics of 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.
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.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass		Malware and other malicious content is blocked before it reaches the network. Our database categorises sites with

	tools as well as sites hosting malicious content		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.
Piracy and copyright theft	includes illegal provision of copyrighted material		The *security.warez* category blocks all sites promoting illegal access and sharing of copyrighted and pirate material. *Forums.p2p* will also block access to all peer-to-peer and file-sharing sites that would enable plagiarism.
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 inappropriate sites such as pornography.
Self Harm and eating disorders	content that encourages, promotes, or provides instructions for self harm, eating disorders or suicide		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.
Violence Against Women and Girls (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.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

Lightspeed Systems outlines its data retention and user identification practices in its privacy policies and trust documentation.

Data Retention Duration
Lightspeed Systems retains data for as long as necessary to fulfill the purposes for which it was collected. After the termination or deactivation of a school account, Lightspeed may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes. However, all student data associated with the school will be deleted in accordance with Lightspeed Systems' Data Deletion policy or in accordance with active Data Processing Agreements (DPA), Data Sharing Agreements (DSA), or Service Level Agreements (SLA).

In certain instances, such as compliance with legal obligations or for business continuity purposes, Lightspeed may retain data for longer periods. For example, system logs are stored for at least 12 months.

Identification of Individuals
Lightspeed Systems collects various categories of personal information that can be used to identify individuals. This includes identifiers such as real name, username, unique user ID, and other similar identifiers. Additionally, device information and connection and usage data, such as IP address, browsing activity, and search terms, are collected.
Access to this information is restricted to authorized personnel and is protected through strict administrative, technical, and physical procedures. Lightspeed Systems employs industry-standard security measures, including data encryption, firewalls, two-factor authentication, and physical-access controls, to safeguard personal information.

For more detailed information on Lightspeed Systems' data retention and privacy practices, please refer to our Privacy Policy and Trust Page here:
https://www.lightspeedsystems.com/en_uk/privacy-policy/

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Using our innovative, patent-pending Smart Agent technology, Lightspeed Systems employs adaptive AI to automatically categorise millions of websites into our expanding database of 138 categories. This robust, education-focused system allows us to accurately classify web content, enabling our clients to tailor web access at a granular level, even down to individual users. This

ensures that students have the necessary access to a wide range of online resources for their learning without facing unreasonable restrictions.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff		Lightspeed Filter has been designed specifically for education. It can be fully customised to perfectly match your organisational structure-tailoring policies based for different year groups, ability, location or for members of staff.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services, DNS over HTTPS and ECH.		Lightspeed's Smart Agents filter any device, any app, any browser; and provide easy SSL decryption without proxies, PACs, or certificate hassles. Our extensive database of URL's is constantly being updated with the latest VPN's and filter bypassing tools and keeping them blocked.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		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. Using Lightspeed Classroom™, teachers can allow or block URLs to expand or constrict access with oversight.
• Contextual Content Filters – in addition to URL or IP based filtering, Schools should understand the extent to which (http and https) content is dynamically analysed as it is streamed to the user and blocked. This would include AI or user generated content, for example, being able to contextually analyse text and dynamically filter the content		Lightspeed Filter utilises a database system that dynamically scans page content to ensure that the page is correctly categorised. Our latest *AI – Detective* category is designed to detect the usage of AI to

produced (for example ChatGPT). For schools' strategy or policy that allows the use of AI or user generated content, understanding the technical limitations of the system, such as whether it supports real-time filtering, is important.		generate content including text analysis, images, video, and more.
● Deployment – filtering systems can be deployed in a variety (and combination) of ways (eg on device, network level, cloud, DNS). Providers should describe how their systems are deployed alongside any required configurations		Our Smart Agents sit on every device and are able to monitor all traffic and provide easy SSL decryption without proxies, PACs, or certificate hassles. For BYOD deployments, a virtual appliance easily installed on your network catches every bit of traffic the Smart Agents can't.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses over blocking		There are more than a billion sites on the web, and thousands are added each hour. Your web filter needs to know them all. The adaptive AI database of Lightspeed Systems leverages AI, machine learning and the infinite cloud for the most accurate and comprehensive categorisation of the Web. This means you save time not having to re-categorise, and you can count on students staying safe without over blocking.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Lightspeed Filter allows tiered levels of control based on user's roles in the organisation, as well as centralised policies that work across entire schools, local authorities or multi-academy trusts.
● Identification - the filtering system should have the ability to identify users and devices to attribute access (particularly for mobile devices) and allow the application of appropriate configurations and restrictions for individual users. This would ensure safer and more personalised filtering experiences.		Lightspeed Filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts. Lightspeed identifies users through a range of different methods including a web portal, agent

		(application) identification, and RADIUS integration.
● 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 filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capability of their filtering system to manage content on mobile and web apps and any configuration or component requirements to achieve this		All traffic that passes through a school or college network can be intercepted, including content via mobile and app technologies. If inappropriate apps are the issue, Lightspeed Mobile Device Management™, utilises app management to control device apps and restrictions.
● 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.
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		Lightspeed Filter use gives schools and organisations the same level of filtering on any device and any OS remotely. Schools can also enable “after school rules” and time or location based policies to these devices to ease restrictions accordingly
● Reporting mechanism – the ability to report inappropriate content for access or blocking		We provide an extensive list of reporting and options to create customised and easily shareable reports.
● Reports – the system offers clear granular historical information on the websites users have accessed or attempted to access		Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group.
● Safe Search – the ability to enforce ‘safe search’ when using search engines		We allow schools to force Safe Search for the entire school or individual groups.
● Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity		The integration of Lightspeed Filter and Lightspeed Alert with CPOMS provides a streamlined approach to safeguarding in schools.

		When Lightspeed Alert identifies a high-concern alert or imminent threat, it automatically transfers this information to CPOMS StudentSafe records. This allows safeguarding teams to manage and customise incidents alongside other records, ensuring that potential risks are addressed promptly. The seamless data synchronisation enhances the ability of schools to monitor student behaviour effectively, enabling staff to respond quickly to any concerns and maintain a comprehensive view of student safety and well-being.

How does your filtering system manage access to Generative AI technologies (e.g. ChatGPT, image generators, writing assistants)?

In your response, please describe whether and how your system identifies, categorises, or blocks Generative AI tools; how access can be controlled based on age, risk, or educational need; any limitations in filtering AI-generated content—particularly where such content is embedded within other platforms or applications; and what support or configuration guidance you offer to schools to help them align with the UK Safer Internet Centre's Appropriate Filtering Definitions and relevant national safeguarding frameworks.

Lightspeed Systems employs a sophisticated approach to identifying and categorising AI technologies. The system utilises a dynamic content categorisation engine powered by AI that proactively classifies billions of URLs before student access. Specific AI-related filtering categories, such as *Artificial Intelligence*, *AI Generative,* and *AI Detective,* have been implemented, leveraging the Smart Agent technology to ensure precise website classification of AI content. Access control is finely tuned through context-appropriate filtering based on age, vulnerability, and risk of harm. This allows for comprehensive visibility and control over digital interactions both on and off the network. Educators benefit from granular customisation capabilities, enabling web access control tailored to individual users. Additionally, Lightspeed Systems includes advanced monitoring capabilities with its AI Notify tool, which provides real-time visibility into student AI usage. This tool generates instant notifications when students navigate to AI websites, empowering educators to effectively monitor and manage AI tool usage in classroom settings. Overall, Lightspeed Systems is committed to ensuring a safe and educational environment for students while managing access to generative AI technologies and references this on various ebooks and guides on our website: https://www.lightspeedsystems.com/en_uk/

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Digital Driver's License for Digital Citizenship: http://iDriveDigital.com Store: https://itunes.apple.com/us/app/idrivedigital/id550609295?mt=8 Google Play: https://chrome.google.com/webstore/detail/ddl/jpohacgnbefbjlgfdpeknggggppkolgdn?hl=en

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

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 & CEO
Date	30th May 2025
Signature