

Appropriate Filtering for Education settings



May 2023

Filtering Provider Checklist Responses

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	July 2023

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
<ul style="list-style-type: none"> • Are IWF members 		<p>Lightspeed Systems has been a member of IWF since 2009.</p>
<ul style="list-style-type: none"> • and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) 		<p>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.</p>
<ul style="list-style-type: none"> • Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		<p>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.</p>
<ul style="list-style-type: none"> • Confirm that filters for illegal content cannot be disabled by the school 		<p>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.</p>

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
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		When a user attempts to search for anything, a list of keywords is referenced. If the search includes any discriminatory or offensive words on the list, access will be blocked. Our importable flagged keyword list contains hundreds of entries, and admins can customise the list with their own keywords that best match their communities.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		We have specific categories for blocking access to <i>drugs</i> and <i>alcohol</i> .
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Our <i>violence.extremism</i> category contains all of 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.
Gambling	Enables gambling		Lightspeed Filter's <i>gambling</i> category blocks all websites related to gambling, casinos, betting, lottery and sweepstakes.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		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.
Pornography	displays sexual acts or explicit images		Naturally all pornographic material in the <i>porn</i> category is blocked. In addition, potentially illegal pornographic material is locked as well as a second category <i>porn.illicit</i> containing potentially illegal pornographic material. This is a sealed category and cannot be unblocked.
Piracy and copyright theft	includes illegal provision of copyrighted material		Our category <i>forums.p2p</i> blocks access to all peer-to-peer and file-sharing sites that would

			enable plagiarism or sharing copyrighted material.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		To prevent any students from looking at websites that promote or display self-harm, again the blocked-search key words is referenced; and a number of different categories can be controlled such as <i>forums</i> and <i>adult</i> . Our safeguarding solution Lightspeed Alert™ built into the 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.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Our <i>violence</i> category contains all sites that promote the use of physical force intended to harm or kill. Lightspeed Alert also notifies schools and admins when students type anything related to violence.

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

Lightspeed Systems uses our online database that leverages AI, machine learning, and the infinite cloud for the most accurate and comprehensive categorisation of the Web. Schools have the ability to restrict access to certain categories or to unknown URLs.

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.

We retain data for as long as necessary to fulfil the purposes for which it was collected for. 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 in accordance with Lightspeed Systems Data Deletion policy, or in accordance with active DPA, DSA or SLA. We may maintain anonymised or aggregated data, including usage data, for analytics purposes.

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

Customers are able to customise the filter to meet their local needs including allowing or blocking categorise, domains, URLs and IPs. Additionally, customers are able to configure the filter to allow normally blocked site for a period of time. Finally, as an education only based company our database is tuned for education by education via our share option where customers can share category changes with us.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff 		<p>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.</p>
<ul style="list-style-type: none"> Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS. 		<p>Lightspeed’s patent-pending 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.</p>
<ul style="list-style-type: none"> 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 		<p>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 Management™, teachers can allow or block URLs to expand or constrict access with oversight.</p>

<ul style="list-style-type: none"> Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter. 		<p>Lightspeed Filter utilises a database system that dynamically scans page content to ensure that the page is correctly categorised.</p>
<ul style="list-style-type: none"> Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking 		<p>There are more than a billion sites on the web, and thousands are added each hour. Your web filter needs to know them all.</p> <p>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.</p> <p>This means you save time not having to re-categorise, and you can count on students staying safe without over blocking.</p>
<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>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 trusts.</p>
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		<p>Lightspeed Filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts.</p> <p>Lightspeed identifies users through a range of different methods including a web portal, agent (application) identification, and RADIUS integration.</p>
<ul style="list-style-type: none"> 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 		<p>All traffic that passes through a school or college network can be intercepted, including content via mobile and app technologies. If</p>

<p>via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps</p>		<p>inappropriate apps are the issue, Lightspeed Mobile Device Management™, utilises app management to control device apps and restrictions.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		<p>Our <i>world</i> 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.</p>
<ul style="list-style-type: none"> Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure) 		<p>Our patent pending 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.</p>
<ul style="list-style-type: none"> 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 		<p>Lightspeed Filter uses patented Smart Agents that sit on every device to give schools 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</p>
<ul style="list-style-type: none"> Reporting mechanism – the ability to report inappropriate content for access or blocking 		<p>We provide an extensive list of reporting and options to create customised and easily shareable reports.</p>
<ul style="list-style-type: none"> Reports – the system offers clear historical information on the websites users have accessed or attempted to access 		<p>Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group.</p>
<ul style="list-style-type: none"> Safe Search – the ability to enforce 'safe search' when using search engines 		<p>We allow schools to force Safe Search for the entire school or individual groups.</p>

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:

Website: <http://iDriveDigital.com>

Store: <https://itunes.apple.com/us/app/idrivedigital/id550609295?mt=8>

Google Play:

<https://chrome.google.com/webstore/detail/ddl/jpohacgnbefbjlgfdpekngggppkolgdn?hl=en>

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	29 TH July 2023
Signature	

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