Appropriate Monitoring for Schools

June 2021

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 they “should be doing all that they reasonably can to limit children’s exposure to the above 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	2nd August 2021

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.

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
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content	🟩	We use 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.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	With solutions built for schools and compatible with every device OS, Lightspeed Systems empowers IT departments and teachers to keep students safe on their digital-learning journeys. Here are two ways we keep our commitment to ending cyberbullying in schools: 1. Our powerful, cloud-based solution Lightspeed Filter allows schools to stop inappropriate behaviour by identifying and remediating high-risk web activity through real-time content analyses and alerts. Set custom flagged terms to better identify phrases and words and drill into individual user activity with our intuitive UI.

		🟩	2. Lightspeed Alert uses advanced AI, real-time alerts, and comprehensive reports to help schools spot the warning signs of cyberbullying. Alert also notifies administrators in real time as it detects potential incidents from any device location. Each notification details the flagged behaviour and provides a link to a complete activity log including screenshots.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet	🟩	To remove opportunities for private exchanges, administrators can block student and/or staff access to forums, instant messaging, web mail and more. Likewise, Lightspeed's MDM, Lightspeed Mobile Device Management™, can prevent inappropriate apps from being installed on school-issued devices, and Lightspeed Filter can alert you of flagged terms being used.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	Lightspeed constantly updates its database of suspicious search terms to help IT staff zero in on discrimination, bullying, gang activity, radical group activity, physical and sexual violence, and more. Not only that, our products can be configured with Trusted Man in the Middle (TMITM) proxy, currently the *only* way to see activity on encrypted (i.e., https://) sites.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	We have specific categories for blocking access to *drugs* and *alcohol* that can be monitored using built-in and custom reports.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Lightspeed helps protect children against extremism by integrating the police-assessed list of unlawful terrorist content into our Filter categories. What is more, advanced reporting features allow IT administrators to easily view Internet activity across the whole school–or drill

		🟩	down to individual users. And email alerts can be set up so suspicious search activity immediately notifies designated staff.
Pornography	displays sexual acts or explicit images	🟩	Schools have the ability to restrict access to certain categories or to unknown URLs. Content associated with explicit sexual acts is always a blocked category.
Self Harm	promotes or displays deliberate self harm	🟩	With Lightspeed Alert, administrators will get real time alerts when students are flagged for words relating to self-harm. The alert provides information including timelines and screenshots, helping administrators quickly investigate severity of incidents. We also have a 24/7/365 in-house team of highly trained safety specialists evaluating all alerts and escalating to school safety personnel and/or the police, enabling early intervention.
Suicide	Suggest the user is considering suicide	🟩	One of the biggest threats to student safety is suicide. It's our mission at Lightspeed Systems to provide tools that not only improve student learning outcomes, but also identify and remediate dangerous online behaviour. Lightspeed Alert immediately flags words relating to suicide. Using advanced AI, it can determine the context of words used and if there is a pattern of this behaviour with specific users, so administrators are only seeing the serious issues.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Our *violence* category contains all sites that promote the use of physical force intended to harm or kill and alerts can be set up when students attempt to access sites in this category.

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.

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 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.

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. 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 has 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 have the ability to 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.
• BYOD (Bring Your Own Device) – if 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, grade level, 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 any and 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 – schools ability to amend (add or remove) keywords easily	🟩	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 of 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.
• 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.
• 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. And when a user is 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.	🟩	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 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.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)	🟩	Lightspeed Filter allows schools to enforce Google safe search which blocks any harmful images students try to access. Our database of over a billion URLs blocks any inappropriate or unknown site ensuring the images are inaccessible.

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

Lightspeed Systems is constantly evolving our software to respond to internet changes to keep children safe. Some recent examples would be Smart Play for YouTube filtering and Lightspeed Alert.

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 & CEO
Date	02.08.2021
Signature	