

Appropriate Filtering for Education settings



June 2016

Provider Checklist Responses

Schools 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”¹. Furthermore, the Department for Education published the revised statutory guidance ‘Keeping Children Safe in Education’² in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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 System
Address	Jubilee House, The Drive, Brentwood, Essex CM13 3FR
Contact details	Darryl LaGace
Filtering System	Lightspeed Web Filter
Date of assessment	June 14, 2016

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.	

¹ Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance_England_Wales_V2-Interactive.pdf

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

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 		Yes
<ul style="list-style-type: none"> and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list) 		Yes
<ul style="list-style-type: none"> Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		Yes

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.		Categories are populated by our crawlers.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Categories are populated by our crawlers.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Category is populate in a sealed category with information received from the Home Office
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Categories are populated by our crawlers and via data received from third parties involved in tracking and stopping Spam, Malware and Hacking
Pornography	displays sexual acts or explicit images		Categories are populated by our crawlers
Piracy and copyright theft	includes illegal provision of copyrighted material		Categories are populated by our crawlers.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Categories are populated by our crawlers.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Categories are populated by our crawlers.

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

This Link applies to all items listed in the above table.

<http://community.lightspeedsystems.com/documentation/web-filter-3/administration/about-our-database/database-categories/> . Additionally all categories are manually reviewed by staff to ensure integrity and calibration of the automated tools.

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"> Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role 		Customers are able to create policies and allow / restrict categories based on their local rules for age and role
<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 		See response above
<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 		The categorisation link above provides details to site classification and categories status as normally allowed or blocked
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		The filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts
<ul style="list-style-type: none"> Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies 		Mobile filtering and app application management are available
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		See world categories
<ul style="list-style-type: none"> Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices 		We provide an inline filtering solution
<ul style="list-style-type: none"> Reporting mechanism – the ability to report inappropriate content for access or blocking 		We provide an extensive list of reporting and

		options to create customised reports
<ul style="list-style-type: none"> • Reports – the system offers clear historical information on the websites visited by your users 		Detailed reporting is available

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”*.³

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>

³ <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	Darryl LaGace
Position	EVP Worldwide Business Development and General Manager
Date	30, June 2016
Signature	