Appropriate Filtering for Education settings

June 2016

Provider Checklist Reponses

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	EIS / Kent County Council
Address	EIS, The Shepway Centre, Maidstone, Kent, ME158AW
Contact details	03000658800
Filtering System	Lightspeed Web Filter
Date of assessment	12/09/2016

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
• Are IWF members		Lightspeed are a member of the Internet Watch Foundation
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Lightspeed automatically block this content
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Lightspeed automatically block this content

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.		They are typically categorized in the Violence.Hate category which we block by default.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		They are categorized into the Drugs category which we block by default.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The Violence.Extremism category is blocked by default.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		These sites are categorized into the Security and Security.Malware categories. Which we block by default.
Pornography	displays sexual acts or explicit images		The Porn and Porn.Illicit are blocked by default.
Piracy and copyright theft	includes illegal provision of copyrighted material		The Forum.P2P category and other categories which cover this content are blocked by default.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Self-Harm websites are categorized into a range of categories, but typically forums.blogs which is blocked by default.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Lightspeed's Violence category is blocked by default.

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

This http://community.lightspeedsystems.com/documentation/web-filter-3/administration/aboutour-database/database-categories/ webpage contains descriptions of Lightspeed standard categories. If websites are incorrectly categorized then schools can either categorize the websites to change the behaviour for their school or contact our service desk and where appropriate we will adjust it for all our schools by recategorizing into one of our 64 custom categories.

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

The default policies which we use for our schools enable access to the majority of websites that a user should be able to access. On the occasion where an over block occurs, the user can contact a school filtering administrator to request that website be allowed. We manage these request for most of our primary schools and where appropriate we recategorize the website into an appropriate category so that the site is no longer blocked for all our users.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		The Lightspeed User Agent (LUA) enables user identification so that different filtering policies can be applied to Users based on Age and Role groups.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		All schools have the option of managing their own Block and Permit policies.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		We have 170 website categories available. 106 website categories are Lightspeed system Defaults and 64 custom EIS categories ensures a great deal of flexibility exists for schools to tailor their schools filtering experiences and policies.
• Identification - the filtering system should have the ability to identify users		This is done via the Lightspeed User Agent (LUA). Users without the LUA can still be identified from the credentials used to access the schools Wireless network or via a Captive Web Portal Page when first accessing the Internet.
• Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		The Lightspeed appliances are inline on egress from our network and will filter mobile and app content in conjunction with our Palo Alto Firewalls.

• Multiple language support – the ability for the system to manage relevant languages		Foreign websites are categorized by Lightspeed into either the standard categories used by English language websites or otherwise into 11 world categories for 11 different languages.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		Lightspeed is deployed inline to egress to the internet to capture all traffic.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Option for Block page to contain text box for sending request for reclassification of website by filtering administrators. Inappropriate content which should be blocked can be reported to Lightspeed via https://archive.lightspeedsystems.com/ or to our Service Desk.
• Reports – the system offers clear historical information on the websites visited by your users		All website access is recorded by Lightspeed and available for Administrators to report upon.

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

KCC provide safeguarding information for schools through http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety and https://kentesafety.wordpress.com/

[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	Richard Packham
Position	EIS Central Services Manager
Date	20/09/2016
Signature