Appropriate Filtering for Education settings

June 2018

Filtering 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" . Furthermore, 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. 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."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

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	Studysafe
Address	Unit 16 Treeton Enterprise Centre, Rother Crescent, Rotherham, S60 5QY
Contact details	Chris Foulstone
Filtering System	Studysafe Managed Solution
Date of assessment	21 December 2018

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		Yes
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Automatically fetch updated lists daily and actively block all entries.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Automatically fetch updated lists daily and actively block all entries.

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.		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Pornography	displays sexual acts or explicit images		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Piracy and copyright theft	includes illegal provision of copyrighted material		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.

Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.
Violence	Displays or promotes the use of physical force intended to hurt or kill		URL blacklists to implement address-level filtering. Weighted phrase lists to implement page content scanning for this content type.

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

Studysafe provides a flexible dashboard for schools and techs to customise their filtering rules. With this additional content filtering any allow or block rule can be easily applied with near instant results. All filtering rules changes are recorded in an audit trail for clear traceability with notes to keep track of why an action was taken.

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

Any over-blocking can be easily and swiftly rectified by applying a simple rule for the blocked resource. The Studysafe team are on hand to help apply any changes should the school tech not wish to make the change themselves.

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		Studysafe provides solutions solely to primary schools and early years, so everything is age appropriate for that age range. Changes can be made by school for any other age ranges as appropriate.
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services		Default routes to the Internet are completely blocked for client devices. Traffic passing through Studysafe, would be blocked by category based rules.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		The dashboard is web-based with a simple approach to adding or amending rules.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Categories are managed on a per group basis. A balanced approach to blocking is applied with content

		scanning used to catch any inappropriate things not outright blocked.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		MATs and school groups are handled both as a single grouped entity and as individual school entities to override where needed.
● Identification - the filtering system should have the ability to identify users		Every request is recorded and reported against a single endpoint and user.
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)		The system operates across all device types and handles all web protocols. Mobile applications that use proprietary protocols or encryption methods would simply fail to function due to network level blocking. Mobile network connections over 4G are not filtered.
● Multiple language support – the ability for the system to manage relevant languages		Multilingual URL lists and phrase lists are implemented
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		The router on site only permits devices to connect to the filtering core, any other requests are blocked at the gateway
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Requests to block or unblock certain content is handled via the support desk or via the school's reseller
● Reports – the system offers clear historical information on the websites visited by your users		Multiple reports are available in the dashboard

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

[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 selfcertification 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	Chris Foulstone
Position	Managing Director
Date	21 Dec. 18
Signature