Appropriate Filtering for Education settings

June 2017

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	Talk Straight Ltd/Schools Broadband
Address	Units 2 – 4 Backstone Business Park, Dansk Way, Ilkley, LS29 8JZ
Contact details	01133 222 333
Filtering System	Lightspeed Systems
Date of assessment	August 2017

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, Schools Broadband and our filtering partners Lightspeed are both members of the IWF
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		This list is fully implemented into the Lightspeed product and site blocked
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This list is fully implemented into the Lightspeed product and site blocked

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.		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block

			activity depending on the school's policy
Pornography	displays sexual acts or explicit images		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy
Piracy and copyright theft	includes illegal provision of copyrighted material		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy
Violence	Displays or promotes the use of physical force intended to hurt or kill		The filter categorises sites, imagery and language relating to this subject. Daily updates are made to over 1 billion categorised entries. The filter enables schools to allow or block activity depending on the school's policy

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

All websites are categorised and schools have the ability to manage which categories they choose to block or allow. Schools can also allow or block individual websites by using URL overrides. Anything not categorised will appear in the unknown list where schools can choose to allow or block.

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

Giving schools direct access to the filters means they can tailor their own browsing experience. We will always provide assistance where required.

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		Schools have ability to set users at different web filter levels generally dictated by age.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		User-friendly interface allows schools to tailor internet access by user, IP, group, organisational unit or domain
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		We recognise today's filters need to provide safe, fast access to valuable educational resources and connections whilst effectively preventing access to inappropriate content. We enable adventurous learning in a safe environment.
• Identification - the filtering system should have the ability to identify users		The filtering system can identify individual users
• 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)		Mobile web browsers are treated in exactly the same way as a traditional web browser. Any mobile device used within the school network undergoes the same filtering as any on-site device. Additionally, we can employ layer 7 application control to further filter or restrict applications.
• Multiple language support – the ability for the system to manage relevant languages		Yes
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		As our filtering System is hosted in our secure data centre, it does not require any additional hardware or software.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Proactive alerts based on the education specific URL database are sent to the school's designated email address/es
• Reports – the system offers clear historical information on the websites visited by your users		Historical data is stored in our secure data centre which

		can be directly accessed and viewed by schools.

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

Online Safety is at the heart of everything Schools Broadband stands for. As online safety is a hugely complex part of what is now a whole school approach, Schools Broadband has a strategic partnership with one of the country's most renowned online safety experts. This partnership gives us access to immediate and up to date advice on all issues relating to "Keeping Children Safe in Education." Our termly newsletter has a regular feature on statutory guidance updates. We also run invaluable and informative online safety seminars for schools offering guidance on how to develop school policies.

[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 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	David Tindall
Position	Managing Director
Date	August 2017
Signature	David Tindall