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	Exa Networks
Address	100 Bolton Road, Bradford, BD1 4DE
Contact details	Mark Cowgill
Filtering System	SurfProtect Fusion
Date of assessment	11th October 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		Yes
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Yes
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Exa is waiting on the CTIRU (Counter Terrorism Internet Referral Unit) list being supplied. Our application for the list was accepted by the Home Office and we are awaiting supply of the latest update from them which will then be integrated immediately into SurfProtect. SurfProtect complies with all prevent requirements and guidelines.

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.		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Pornography	displays sexual acts or explicit images		In line with DfE guidelines, SurfProtect has website, content

			and URL categorisation, which by default is actively enabled to deal with this content
Piracy and copyright theft	includes illegal provision of copyrighted material		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content
Violence	Displays or promotes the use of physical force intended to hurt or kill		In line with DfE guidelines, SurfProtect has website, content and URL categorisation, which by default is actively enabled to deal with this content

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

SurfProtect uses proprietary in-house developed software and libraries continually developed over the past thirteen to categorise websites and content to help ensure that inappropriate material is categorised correctly and restricted where required.

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

SurfProtect uses proprietary in-house developed software and libraries continually developed over the past thirteen to categorise websites and content to help ensure that inappropriate material is categorised correctly and restricted where required. Our end users also have the ability in real time to recatagorise any URL or part of to another category if required, or just allow part of a site, for instance a specific video on YouTube as opposed to opening the whole site.	

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		SurfProtect fusion integrates with Active Directories or other authentication or radius services to ensure that schools can provide age appropriate filtering on a granular level, from across the whole school,

		to per user, to per machine.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		SurfProtect Fusion has an intuitive cloud interface that allows real time access to the system to override allowed or blocked sites as required. Only the IWF and CTIRU (when applicable) cannot be bypassed, in line with DfE guidelines.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Full guidelines on this can be found on www.surfprotect.co.uk
• Identification - the filtering system should have the ability to identify users		Yes, per user and/or per machine.
• Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		Yes, SurfProtect Fusion has application control.
• 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		No software is installed on users devices. SurfProtect is a network level service
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Yes.
• Reports – the system offers clear historical information on the websites visited by your users		Yes

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

Exa launched the Exa Foundation, more information can be found by visiting www.exa.foundation to help schools specifically with difficult or challenging matters such as e-safety training and guidance as well as other related topics such as Computer programing/curriculum. The Foundation is entirely free for all Exa schools.

[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

Name	Mark Cowgill
Position	Co-Founder & Director
Date	12th October 2016
Signature	