Appropriate Monitoring for Schools

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 monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	Exa Networks
Address	100 Bolton Road
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

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		Yes
• Work with CTIRU '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) to supply the update content. SurfProtect complies with all prevent requirements and guidelines.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Child Sexual Exploitation	: Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed

Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Pornography	displays sexual acts or explicit images		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Self Harm	promotes or displays deliberate self harm		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through

			SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Suicide	Suggest the user is considering suicide		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
Violence	Displays or promotes the use of physical force intended to hurt or kill		SurfProtect uses proprietary in-house developed software to catagorise websites and content to help ensure that inappropriate material is catagorised correctly and restricted where required. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed

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 to catagorise websites and content to help ensure that inappropriate material is catagorised 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 to catagorise websites and content to help ensure that appropriate material is catagorised correctly and allowed where required.	

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to		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. Schools have access through SurfProtect Fusion a collection of reports and tools to see what content has been attempted to be accessed
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported?		SurfProtect Fusion is deployable across all parts of a schools networks, including WiFi for pupils or staff with BYOD. This is in line with DfE guidelines. SurfProtect Fusion is not applied to devices not connected to Exa or the schools network as this is network level filtering (in line with DfE Guidelines) and not software installed on each device.
• Data retention –what data is stored, where and for how long		Data on usage is stored in one of Exa's multiple Datacentres in the UK for up to one year. Schools can download the full logs and files for longer retention if required.
• Flexibility – schools ability to amend (add or remove) keywords easily		Yes, SurfProtect Fusions intuitive control panel allows this to be done instantly.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		We do not advise end users of the monitoring, this is the responsibility of the organisation using SurfProtect. We also provide training through the Exa Foundation and free resources on www.surfprotect.co.uk
• Multiple language support – the ability for the system to manage relevant languages?		Yes

• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		SurfProtect alerts are in the form of the online reports, which schools have access to 24/7. Email notification alerts are to be introduced in the near future.
• Reporting – how alerts are recorded within the system?		Within the reporting tools. SurfProtect is a filtering system first and foremost with monitoring capability it is not a dedicated monitoring service such as Securus or Future Digitial. Reporting, which is different to Alerts are all via the reporting interface.

Please note below opportunities to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

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.

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	