Appropriate Filtering for Education settings

May 2023

Filtering Provider Checklist Reponses

Schools (and registered childcare providers) 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, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

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 and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's 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 Ltd
Address	100 Bolton Road, Bradford BD1 4DE
Contact details	Emily Ruthven
Filtering System	SurfProtect
Date of assessment	06/06/2023

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 we are IWF members
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		We actively implement the IWF URL list to block access to illegal child abuse images
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		We have integrated the police assessed list of unlawful terrorist content produced on behalf of the Home Office
• Confirm that filters for illegal content cannot be disabled by the school		Filters for illegal content cannot be disabled by the school

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.		Please see below wording under the table which explains how content is managed through our filtering system.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Please see below wording under the table which explains how content is managed through our filtering system.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Please see below wording under the table which explains how content is managed through our filtering system.
Gambling	Enables gambling		Please see below wording under the table which explains how content is managed through our filtering system.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Please see below wording under the table which explains how content is managed through our filtering system.
Pornography	displays sexual acts or explicit images		Please see below wording under the table which explains how content is managed through our filtering system.
Piracy and copyright theft	includes illegal provision of copyrighted material		Please see below wording under the table which explains how content is managed through our filtering system.

Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Please see below wording under the table which explains how content is managed through our filtering system.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Please see below wording under the table which explains how content is managed through our filtering system.

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

Key word filtering is used to identify a search query through the use of search engines. Exa provides a curated key word list to all customers as a default, customers can then add their own additional words/sites for anything else they want to block.

When a website is visited for the first time Exa will categorise the website, for all these content types we will automatically block them. For any others the schools can choose to block. Exa will periodically sample the list to see if the content needs to remain on the blocked list.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

As specified in the contracts for SurfProtect, if customers have SurfProtect Quantum logs are guaranteed to be kept for 3 months, and with SurfProtect Quantum+ are guaranteed to be kept for 1 year.
The identification data held is dependent on what each customer sets usernames up as (eg if the school uses first name and last name, or student ID numbers etc. we will have that information).
Data is only accessible internally to Exa by authorised personnel who need it for their job roles.

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

Exa have a default set up for customer profiles which has lists of content already blocked. Individual customers can then tailor the lists to their own needs, enabling and disabling content as required with the exception of the illegal content as mentioned at the start of this question set, this content is unable to have the filter removed.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm –		Exa provide default profiles as a standard set up,

also includes the ability to vary filtering strength appropriate for staff		customers can then create different user groups and filter by levels as required
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		We can filter DNS over HTTPS VPN/Proxy is being worked on, plans are being made for how we can filter. We do filter embedded URLs to determine if they include something which should be blocked. We also can use advance firewall traffic detection to block traffic profiles such as VPN should the customers take our firewall product.
● Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		Exa provide default profiles as a standard set up, customers can then create different user groups and filter by levels as required. Audit logs are kept for who has made changes. Schools can only make changes to their own profiles.
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter.		We do this on searches on the first time a search is made, then as and when they come up as part of the sampling reviews. We would filter all search results for blocked content not just the exact URL they are trying to reach
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		We don't have a documented Filtering Policy, however all filtering information is available through the website - https://exa.net.uk/content-filtering-surfprotect/
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		As standard all sites are set up the same, where changes are required the customer can request these and they can be deployed to all sites.
● Identification - the filtering system should have the ability to identify users		As long as the customers are using a method of filtering

		which is possible for us to identify users then we can
• 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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps		Exa filter content at a network level rather than device, filtering is done on app, mobile, browser etc.
• Multiple language support – the ability for the system to manage relevant languages		The blocklist is multilingual the organisation will soon publish the list of languages we block.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		All filtering is applied at network level
• Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		Quantum+ service using VPN or captive portal applies filtering on remote devices
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Customers can send tickets into Exa or can change their own filtering settings
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		Activity logs are generated and customers can access their own logs
• Safe Search – the ability to enforce 'safe search' when using search engines		If the search engine provides safe search we have the ability to enforce it

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

In addition to our content filters and accompanying tools, schools also take advantage of our comprehensive education programme through The Exa Foundation [http://exa.foundation]. Established in 2015, the Foundation provides schools with interactive and engaging workshops for children, high quality CPD training for staff and valuable information sessions for parents. Our Learning Programme addresses specific themes related to online safety and protection enabling participants to become better informed users of connected technologies and reduce their exposure to risks.

[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	Emily Ruthven
Position	Information Governance Manager
Date	27/06/2023
Signature	E.Ruthven