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	**Censornet Ltd**
Address	**Matrix House, Basing View, Basingstoke, RG21 4FF**
Contact details	**Gareth Lockwood, VP Product, gareth.lockwood@censornet.com**
Filtering System	**Censornet USS – Web Security Advanced**
Date of assessment	**24/10/2023**

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	🟧	Indirect member: zVelo Inc who provide our Web URL classification and analysis analysis have been a member since 2011.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	Our OEM partner zVelo implement the IWF list and automatically integrate into our Web security classification engine.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	CTIRU option is enabled for education and public sector clients.
● Confirm that filters for illegal content cannot be disabled by the school	🟩	Default System Rules cannot be deleted. RBAC facilitates read-only access to Filter Rules.

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.	🟩	Defined as extreme right and/or left wing groups, sexist remarks, racist remarks or racial slurs, religious hate, or the promotion of oppression of certain groups or individuals based on race, religion, nationality, political affiliation, gender, age, disability, or sexual orientation.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Defined as pages that in any way endorse or glorify commonly illegal drugs, the misuse of prescription drugs, the misuse of inhalents, or any positive references to the culture of drug use whether specific drugs are mentioned or not. Includes sites giving non-clinical descriptions or stories about being high as well as blogs and other posts about getting high. Separate sub-category for Marijuana. Does not include Government owned sites.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Deep inspection of Social Media apps like Facebook, Twitter

		🟩	including keyword reporting; Web categories Hate Speech and Violence (described as Web pages that promote questionable activities such as violence and militancy)
Gambling	Enables gambling	🟩	Category includes Games that involve the winning or losing of money based on strategy and chance. Includes information, tips, strategies, and rules for gambling games.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	"Web pages with information or tools specifically intended to assist in online crime such as the unauthorized access to computers, but also pages with tools and information that enables fraud and other online crime. Also includes phone system hacking (aka phreaking). Note that computer security testing tools that don't result in the actual compromise of a computer belong in the *Information Security* category. Examples are phreaks, root kits etc. Web Categories include: Malware CallHome, Malware Distribution Point, Phishing/Fraud, Hacking. An integrated anti-malware module is included from Bitdefender to scan files and content.
Pornography	displays sexual acts or explicit images	🟩	Safe Search enforcement and Web Categories: Pornography, Sex & Erotic, R-Rated. Optional Image Filter module provides real time image scanning for pornographic content
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Web category Piracy & Copyright Theft, described as Web pages that provide access to illegally obtained files such as pirated software (aka warez), pirated movies, pirated music, etc. Web Category: Torrent Repository, described as Web pages that host repositories of torrent files, which are the instruction file for

		🟩	allowing a bittorrent client to download large files from peers
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Web Category Self Help & Addition, described as Web pages which include sites with information and help on gambling, drug, and alcohol addiction as well as sites helping with eating disorders such as anorexia, bulimia, and overeating
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Web Category Violence described as Web pages that promote questionable activities such as violence and militancy

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

- □ Full visibility of Cloud Application usage and Social Media sites including capturing actions such as posting to social network sites and search engine terms
- □ Scans all accessed URLs for reputation based on Web Category
- □ On-demand lookup for unknown URLs / zero-day
- □ Integrated Anti-malware scanning
- □ MIME Type Scanning
- □ Counter Terrorism list enforcement
- □ Safe search enforcement – Google Safe Search, Google App Domain, Bing, Yahoo!, YouTube, YouTube for Schools
- □ Policy based control of Web categories and Safe Search
- □ Keyword lists to trigger policies, i.e. profanities, radicalisation. DLP module to filter based on file contents.

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.

Default is 90 days with auto-archive to CSV which is available for a further 12 months free of charge. The 90 day retention period can be extended for an extra free.

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

- □ Blocking is applied through policy, either globally or down to user group, individual or device level
- □ Default option for blocking any unclassified sites
- □ All system categories can be overridden with custom URL category entries
- □ Unblock Request management system alleviates IT helpdesk overhead and streamlines requests to unblock web content

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 – also includes the ability to vary filtering strength appropriate for staff	🟩	Rules can be applied based on AD attributes; username, OU, group, device and the rules determine what content is blocked. Rules can also be set based on time of day
● 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.	🟩	Web Categories that detect anonymizer (proxy) sites, different deployment options such as explicit proxy, transparent proxy, endpoint agent provides flexibility in different environments
● 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	🟩	Web based control panel with roles based access. Full control to manage content blocking settings. Full audit log to track administrator changes.
● 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.	🟩	Full inspection and filtering of SSL encrypted traffic over https. Content can be scanned and Administrators/Safeguarding staff can review the blocked activity and any search/keywords using the integrated log viewer to determine the context.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	CensorNet's web filtering policy and approach is published at http://help.clouduss.com/censornetweb-filtering-policy-approacheducation and includes a link to a complete list and description of more than 500 categories. Critically CensorNet offers page level categorisation and a range of features specifically developed for education over the last 10+ years
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Centralised configuration, management and reporting via a single dashboard with enforcement on network or device level using gateway (VM's) or endpoint agents. Global network infrastructure ensures low latency web browsing

● Identification - the filtering system should have the ability to identify users	🟩	Active Directory/AzureAD integration and optional IDaaS module.
● 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	🟩	This is achievable via a Captive Portal mechanism when the device is on the local network, or via VPN to the gateway for roaming users (requires MDM solution). In addition, we offer a Cloud Application Security module which has an App Catalog of hundreds of mobile and desktop apps that can be used to identify apps in use and control access to them.
● Multiple language support – the ability for the system to manage relevant languages	🟩	Over 100 languages are supported in the URL database
● 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)	🟩	Gateway software is available which can act as an explicit or transparent proxy
● 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	🟩	Hybrid deployment model including gateways and device-based agents to secure both on-premise and remote users. Policies can be applied based on user/role/device with options for different rules for remote/onsite access.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Extensive Web Activity audit reports and pre-defined charts
● Reports – the system offers clear historical information on the websites users have accessed or attempted to access	🟩	Historical logs are available for up to 90 days and then via a downloadable archive
● Safe Search – the ability to enforce 'safe search' when using search engines	🟩	

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 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	Gareth Lockwood
Position	VP of Product
Date	24/10/2023
Signature	