Appropriate Filtering for Education settings

September 2019

Filtering 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	Censornet Ltd
Address	Matrix House, Basing View, Basingstoke, RG21 4DZ
Contact details	Tim Lloyd
Filtering System	Unified Security Service – Web Security
Date of assessment	18/09/2019

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		We are indirect members via zVelo Inc who provide our URL classification service
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU option is enabled for education/government customers

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.		Web category Hate Speech described as: Web pages that promote extreme right/left wing groups, sexism, racism, religious hate and other discrimination
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Web category Illegal Drugs described as: Web pages that promote the use or information of common illegal drugs and the misuse of prescription drugs and compounds
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)
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Web Categories: Malware Call-Home, Malware Distribution Point, Phishing/Fraud, Hacking Optional BitDefender gateway AV module.
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	includes illegal provision of		Web category Piracy & Copyright

copyright theft	copyrighted material		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 over-eating
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
- Anti-malware scanning
- Image Filter scanning
- Counter Terrorism list enforcement
- Safe search enforcement – Google search, Bing, Yahoo!, YouTube
- Policy based control of Web categories and Safe Search

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

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 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
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		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		Web based control panel with roles based access. Full control to manage content blocking settings
• 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 here http://help.clouduss.com/censornet-web-filtering-policy-approach-education 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
• 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		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

filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		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		Gateway software is available which can act as an explicit or transparent proxy
● 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 visited by your users		Historical logs are available for up to 90 days and then via a downloadable archive

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	Tim Lloyd
Position	Head of R&D
Date	18/09/2019
Signature