Appropriate Filtering for Education settings

April 2023

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*" and they "should be doing all that they reasonably can to limit children's exposure to the above 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."

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	Renato Software Ltd.
Address	Sterling House, Wheatcroft Business Park, Edwalton, Nottingham, NG12 4DG
Contact details	0115 857 3776 m.payne@renatosoftware.com
Filtering System	Senso Content Filtering
Date of assessment	20/04/2023

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		Senso is a member of the IWF and actively communicates with them.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		IWF Lists are provided and updated within Senso via an API.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU URL Lists are provided and updated in real time within Senso via an API.

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.		The discrimination category is one of 500+ unique web filtering content categories available to Senso, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy. The selection of active categories is made based on the needs of our users.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs and Substance Abuse as above.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Extremism is covered as above, plus real-time daily updates of the CTIRU URL lists.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Malware and hacking are covered by the Malicious Internet Activity category.
Pornography	displays sexual acts or explicit images		Pornography and adult content are covered by a number of categories.
Piracy and copyright theft	includes illegal provision of copyrighted material		Piracy and copyright theft are covered by the Criminal Activity / Piracy categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Self-harm is covered by a dedicated self-harm category.

Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons and violence are covered by dedicated categories.

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

The Senso Content Filtering has the capability to filter against 500+ unique content categories, with more than 99% active web coverage and accuracy. More than 200 languages are supported and it receives daily and real-time updates.

Senso's Content Filtering not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries.

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.

We have a basic filter package which doesn't include logging of internet history, and a premium package which includes logging of internet history. The latter retains logs from the date of installation for the length of a customer's active subscription.

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

Senso as a provider work closely with partners and customers to ensure the filter is appropriately blocking harmful and inappropriate content without over-blocking. Customers have the option to both schedule and turn off completely specific categories such as social media and gaming, based on age or role within the school, to allow for a flexible and strategic approach to internet use. Senso also provides the ability to whitelist any websites which are blocked by Senso Content Filtering on the fly, as required by the individual customer.

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		Senso Content Filtering can: - Schedule all/some categories - Group web-filtered users by criteria such as staff / year group with options to allow certain categories at certain times and have different strengths of filter.

• 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.		Senso blocks access to torrent repositories, proxy anonymisers, and peer-to-peer file-sharing sites to help prevent circumvention.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Senso has the ability to add wildcards, words or URLs to the filter as required. Filter categories can be turned on and off, and URLs can be whitelisted.
• 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. For example, being able to contextually analyse text on a page and dynamically filter		Senso's Content Filtering uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Senso maintains a document which details what content should be in which category, as well as a detailed factsheet on the approach the web filter takes. Senso's Content Filter combines AI with human assessment to maintain over 99% accuracy of web filter categories. The present document can be taken as our rationale on filtering and overblocking.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Senso Content Filtering is scalable and flexible to support multi-site management from the top level right down to individual user-specific filtering policies.
• Identification - the filtering system should have the ability to identify users		Users are identified when they log on to the device.
• 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)		Senso Content Filter implements market-leading web filtering across all Chrome-based web apps, and Senso also offers a specific app for iOS which replaces the Safari browser to enable comprehensive web filtering. For all other

		non-browser web apps we strongly recommend using an MDM solution that restricts apps that gain access to the internet.
• Multiple language support – the ability for the system to manage relevant languages		More than 200 languages are supported.
• 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)		In response to the increase in remote teaching and learning, Senso is entirely cloud-based and as such does not require on-premise network filtering infrastructure. This means that it can support devices whether they are on or off the school network.
• Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school		Senso is a cloud-based solution which means that there is no difference in filtering quality whether a device is in school or elsewhere. If preferred, there is the option to schedule the Senso Filter Cloud to turn on once a device leaves the network or at specific times.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Senso has a section called 'Concern Reports' which is a record of all manually reported sites. We are currently working on implementing a user-driven reporting mechanism for reporting inappropriate content.
• Reports – the system offers clear historical information on the websites visited by your users		In the premium Content Filtering package, all websites visited by users are logged within Senso.

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]

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Please note below opportunities to support schools (and other settings) in this regard

Senso offers its existing customers a free Learning Management System (**Senso Learn**) through which school staff members, of all roles, can take specific Safeguarding courses in order to best support children in keeping safe online as well as in the classroom.

Other ways Senso can support schools with Safeguarding:

Senso Safeguard Cloud

Senso Safeguard Cloud offers cloud-based, real-time monitoring of activity on school-owned devices, designed to highlight to school staff users who may be vulnerable, a risk to themselves, a risk to others, or behaving inappropriately. Senso indicates a potential concern by raising a "violation" when a keyword, acronym or phrase types by a user matches against those found within our libraries. The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding portal user. The screenshot will also be analysed by our AI-driven image analyser to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed; this helps with prioritisation of Senso violations. Senso Safeguard Cloud integrates with CPOMS & MyConcern to support seamless reporting, and has a live dashboard to facilitate proactive and strategic online safeguarding. Users can also anonymously report a concern about themselves or someone else and include a screen capture if required.

Senso Safeguarding for Microsoft Teams App

Senso has the capability to monitor all Microsoft Teams Chat regardless of the device or location of a user. Senso Teams monitoring also analyses images alongside the text chats to identify high-risk users or behaviours. Violation information, including chat transcripts, can then be viewed in the dashboard by the relevant Senso Safeguarding portal user. All images sent within Microsoft Teams chat are also analysed by our AI driven image analyser to indicate whether a student is potentially sending harmful or inappropriate images.

Senso Safeguarding Assisted Monitoring Service

Senso users may also opt to benefit from our assisted monitoring service with human screening/moderation of violations, including external escalation and real-time evaluation of events by safeguarding experts. Effective triage, including phone calls for the most serious cases, means that user violations receive the appropriate level of attention.

Senso Class Cloud

Senso's classroom management software enables teachers to take control of the class and keep students focused on a task, whether the class is taking place in person or online. Teachers can actively monitor students' activity, send messages directly to devices, take control of devices, and lock users' screens for safety and attention purposes.

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	Michael Payne
Position	Director of Operations
Date	28-Apr-2023
Signature