

Appropriate Filtering for Education settings

May 2023

Filtering Provider Checklist Responses

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	Securly
Address	Third Floor One London Square, Cross Lanes, Guildford, Surrey, United Kingdom, GU1 1UN https://www.securly.com/
Contact details	uksales@securly.com 0141 343 8322
Filtering System	Securly Filter and Aware
Date of assessment	3rd August 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
<ul style="list-style-type: none">Are IWF members		Securly is a current member of the Internet Watch Foundation and has been since 01/03/2016.
<ul style="list-style-type: none">and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		All Securly customers are blocked access to the IWF CAIC list of domains and URLs which host illegal child abuse content.
<ul style="list-style-type: none">Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Securly integrates and blocks unlawful terrorist content using the list provided by the UK Home Office and Met Police CTIRU (Counter-Terrorism Internet Referral Unit).
<ul style="list-style-type: none">Confirm that filters for illegal content cannot be disabled by the school		Securly Filter cannot be disabled by the school. All illegal content categories are locked at a system level. Schools cannot disable these filters.

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.		Securly provides a “Hate” category which allows administrators to block access and alert on websites and content which promote hatred and discrimination across race, religion, age, or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Securly provides a “Drugs” category which allows administrators to block access and alert on websites and content which includes details of manufacture, sale, distribution, and recreational use of illegal substances.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Securly includes the Home Office / Met Police CTIRU illegal terrorist content blocklist and provide a “Hate” category. This allows administrators to block access and alert on websites and content which promotes terrorist organisations and actions, violence, and intolerance.
Gambling	Enables gambling		Securly provides a “Gambling” category which allows administrators to block access and alert on websites and content that promotes betting or risky actions for a reward.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Securly provides a “Network Misuse” category which allows administrators to block access and alert on websites such as VPNs, the Tor network, known malware hosts, C&C servers, and anonymous proxy servers which would allow bypass of filtering or potential harm to a school network.

Pornography	displays sexual acts or explicit images		<p>Securly provides a “Pornography” category which allows administrators to block access and alert on websites that display sexual acts or explicit images.</p>
Piracy and copyright theft	includes illegal provision of copyrighted material		<p>Securly provides a “Streaming Media” category to restrict access to streaming media providers.</p> <p>The “Network Misuse” category will restrict access to common filesharing platforms.</p> <p>Enforced “Creative Commons” mode can be enabled for image search to limit results to only those available under the Creative Commons license.</p>
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		<p>Securly Aware uses AI sentiment analysis to detect self-harm content, emails, web searches and social media posts.</p> <p>Alerts are categorised under the terms ‘Self-harm’ and ‘Grief’</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>
Violence	Displays or promotes the use of physical force intended to hurt or kill		<p>Securly Filter and Aware uses AI sentiment analysis to detect violent content, emails, web searches and social media posts.</p> <p>Alerts are categorised under the terms ‘Violence’</p> <p>Securly will flag activity from vulnerable students in real-time to enable emergency intervention.</p>

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

- Audit logs. Keeps a record of each instance when an admin or teacher allows a site.
- Securly Filter categories include keywords/phrases, URLs and domains of over the top one million websites globally and growing.
- Securly PageScan, using AI and human moderation, provides automated categorisation of previously unknown websites by scanning page content and images.
- Selective HTTPS man-in-the-middle decryption provides real-time dynamic URL filtering, keyword filtering and sentiment analysis.
- Our customers can provide their own block and allow lists in policies and can submit any websites for inclusion in our categories.
- Securly can transparently proxy select websites on demand, allowing us to detect cyberbullying, suicide, and violence, on social media websites such while providing fast URL filtering on the rest of the traffic—on any device, anywhere.
- Take-home policies. Devices that go home can easily have separate policies based on location, rather than time-based roles – these policies automatically change when the device is back on a school network.
- Delegated admins can control policies that are associated with the pupils they have visibility of, ideal for multi-academy trusts who want to give control out to schools whilst maintaining overall management.
- With Securly Home (an add-on for Filter) parents can view their child’s recent searches, sites visited, and videos watched on their school-owned device depending on the level of control set by the school.

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.

All customer log data is stored securely within Securly's servers for a minimum of 1 year as standard. Customers can discuss their individual retention requirements if this is unsuitable.

Activity logs are stored in AWS EU-West-2 (London). There is some processing done on EU-West-1 (Dublin) for the dashboard and any scheduled reports. Our support team is around the world and may access your data as part of a support ticket, but it will remain in the UK.

To ensure the ongoing availability of critical data, management has established a schedule of backups and data redundancy. Backups and replications are monitored for failures, and resolved in a timely manner.

Securly has achieved SOC2 Type 2 certification, demonstrating a commitment to data security and responsibility.

Backups of production databases are performed based on the database type:

- Configuration - daily full snapshots/AMI backups and retained for 7 days
- Logs - monthly backups retained for one month.
- Data is replicated across geographically separate availability zones.
- Backups and replications are monitored for failures. In the event of three successive nightly failures, IT will open an incident ticket to investigate the issue.
- IT performs restorations of data per customer or business requests. System restore capabilities are tested at least annually.

[How Does Securly Comply with GDPR?](#) For information about GDPR or if you have any questions about our GDPR compliance, please contact us at support@securly.com

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

Unlike traditional on-premise filtering solutions, Securly will selectively intercept web traffic to block and filter content. This prevents over blocking or problems accessing safe content and education applications.

Previously unknown or uncategorised websites will be analysed by Securly PageScan to accurately determine their category and if they need to be filtered.

Administrators also have ability to manage their own safe sites and override Securly categorised websites.

[How does temporarily allow sites work?](#)

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff 		<p>Securely Filter is built exclusively for education and has school appropriate filtering configured out-of-the-box and allows easy configuration of more strict or relaxed policies as required.</p> <p>Securely Filter includes the ability to generate instant alerts for blocked content. This is configurable at a policy level to allow for different alert levels for vulnerable users.</p> <p>Securely can be configured to define separate filtering policies appropriate to different age groups or roles. E.g. Staff, Primary School Students, Senior Students, Criminology Students, etc.</p>
<ul style="list-style-type: none"> 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. 		<p>Securely works with schools to ensure Securely Filter is applied in the most robust way possible and includes publicly available best practice guides and recommendations for configuring devices and networks to best protect children and prevent circumvention.</p> <p>Securely provides a “Network Misuse” category to prevent access to websites that provide proxy circumvention services or VPNs.</p> <p>Securely publishes best practice guidance on how to help prevent circumvention.</p> <p>Securely MDM and Classroom can help restrict access to applications, and allows teachers to monitor student devices.</p>
<ul style="list-style-type: none"> 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 		<p>Securely administrators can permit or deny access to content by using their own domain names and keywords globally or per policy.</p> <p>Staff members assigned to Faculty Groups can edit policies that affect OUs or Security Groups assigned to them. This feature can be enabled and disabled at an admin level.</p>

		<p>Any substantial changes to the system are logged in an audit trail.</p>
<ul style="list-style-type: none"> 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. 		<p>Securly Filter and it's classification engine PageScan looks at content of new sites to determine an appropriate category. For sites that have little or no metadata to interrogate, Securly PageScan processes images within a site and will classify as Pornography if ANY of the images are perceived to contain nudity, this is an automated process.</p> <p>Securly can filter SSL traffic, providing full protection and customisation as necessary, while only decrypting websites under our blocked categories, leaving other sites alone. This helps eliminate latency, and allow full scalability while taking care of HTTPS traffic.</p> <p>Securly Aware is able to monitor chat logs and posts that are submitted to selected sites, such as ChatGPT, TikTok, Twitter, Facebook, Instagram.</p>
<ul style="list-style-type: none"> Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking 		<p>Securly publishes details of its filtering approach and rationale on the publicly available knowledgebase.</p> <p>More information on Securly PageScan technology can also be found on our tech blog.</p>

<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>As a cloud-based service, Securly Filter and Aware are available anywhere with Internet access.</p> <p>Delegated control can be provided to additional administrators or Safeguarding teams.</p> <p>Multiple sites and take-home policies can all be managed from the same central dashboard.</p> <p>For large school trusts or partners managing filtering for multiple schools, Securly’s Multi-School Dashboard provides a dropdown that lets the admin switch across different schools without having to log in separately each time.</p> <p>All activity is also logged in the Audit log for that specific school and can be viewed by the school admin in the Multi-School view.</p>
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		<p>Securly Filter can be applied to managed browsers, and managed devices, with user-level logging and filtering through sign-in with Microsoft Azure/EntraID or Google G-Suite.</p> <p>Securly integrates with Microsoft Azure AD/Entra ID, Windows Server Active Directory, and Google G- Suite to provide user identification.</p> <p>Activity reports contain detailed information about the activity selected for specific users or OUs, including:</p> <ol style="list-style-type: none"> 1. The student and OU/Group names 2. Type of activities that are listed in the report. This depends on what type of activities you select when downloading the report. 3. Policies for which the report is generated. 4. Categories for the activities that are listed. 5. Whether activity has been Allowed, Blocked or Flagged. 6. The date and time stamp of each of the events is listed in each of the rows.

<ul style="list-style-type: none"> 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 		<p>Securly Aware connects directly to Microsoft Office365 and G-Suite Workspace to scan documents, emails, chats, images, and videos for inappropriate content regardless of where those systems are used or how they are accessed.</p> <p>Securly Filter is a best of breed web filter, however, as some apps communicate using non-HTTP/HTTPS protocols or prevent interception of traffic using end-to-end encryption, this may cause applications to bypass filtering, break or experience unexpected behaviour.</p> <p>We strongly recommend Securly Filter be combined with mobile device management such as Securly MDM to ensure only appropriate applications can be installed.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		<p>Securly implements multiple language support for both filtering and management interface in English, French, and Spanish.</p> <p>Language support is being continually developed and additional languages will be added as available.</p>
<ul style="list-style-type: none"> 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) 		<p>As Securly is cloud based it can be implemented at the 'network level' using DNS or network settings and does not require software deployed on devices.</p>
<ul style="list-style-type: none"> 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 		<p>Securly Filter can be applied to school owned devices regardless of how they access the internet or whether they are within the school network.</p> <p>Securly Filter can also be applied to BYOD schemes, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.</p>

<ul style="list-style-type: none"> Reporting mechanism – the ability to report inappropriate content for access or blocking 		<p>The Securly block page can be configured to allow staff or students to request sites from the admin.</p> <p>Customers can also make manual submissions via our website.</p> <p>End users also can be provided with a link to submit feedback to administrators.</p>
<ul style="list-style-type: none"> Reports – the system offers clear historical information on the websites users have accessed or attempted to access 		<p>Securly has designed reports and alerts to be delegated to school management and safeguarding teams to allow quicker response to incidents.</p> <p>Reports are designed with schools in mind and make visually clear which sites are accessed or blocked. Additionally, searches, videos, and social media content are also highlighted.</p> <p>Filters can be applied by user, date/time, category and policy.</p>
<ul style="list-style-type: none"> Safe Search – the ability to enforce ‘safe search’ when using search engines 		<p>Safe Search can be applied on a policy group basis.</p>

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>

Securly's filtering policies are customisable and policy changes can be applied to specific user groups by the administrator, so that over blocking doesn't occur for certain student groups if they are researching legitimate areas to do with sexual health for due to the requirements of the RHSE and PSHE curriculum.

Securly's primary aim is to enable schools and Multi Academy Trusts to make web experiences safer for students every day. To this end, Securly is committed to partnering with their schools to support and enhance the online experience and deliver a healthy and safe digital environment for all students.

Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsibility digital citizenship. Think Twice, prompts students to reconsider before they send hurtful messages.

Wellness Widget Intervention. When a student's Wellness Level drops, the Wellness Pathways widget will automatically present helpful resources to them on their screen.

Securly are a Student Safety company and are concerned with wellbeing of students beyond web filtering;

- [Securly Aware](#) - Student safety and wellness solution that provides unprecedented visibility into your students' mental health and wellness. Google Drive files, One Drive files, emails, social media, and web searches are scanned to identify indications of suicide, depression, violence, bullying, and nudity.
- [On-call](#) - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now
- [Securly Home](#) - Parent app, a free feature included with your school's Filter purchase, giving parents control over their child's school device when it goes home, including web filtering, site restrictions, and monitored screen time.
- [Classroom](#) - Classroom management tool that works seamlessly across Chrome, Windows, and Mac.
- [MDM](#) - Cloud-based Apple device management for 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
- 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	Jarrett Volzer
Position	VP of Product
Date	03/08/2023
Signature	