Appropriate Filtering for Education settings

June 2020

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	Securly
Address	Securly EMEA, 24 Speirs Wharf, Glasgow, G4 9TG
Contact details	https://www.securly.com/contact-us
Filtering System	Securly:// Filter, Auditor, 24
Date of assessment	25th June 2020

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	🟩	Securly is a current member of the Internet Watch Foundation.
● 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.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Securly integrate and block unlawful terrorist content using the list provided by the UK Home Office and Met Police CTIRU (Counter-Terrorism Internet Referral Unit).

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 provide 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 provide a "Drugs" category which allows administrators to block access and alert on websites and content which include details of manufacture, sale, distribution, and recreational use of illegal substances.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Securly include 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 include promote terrorist organisations and actions, violence and intolerance.

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	Securly provide a “Network Misuse” category which allows administrators to block access and alert on websites such as VPN, Tor Networks, known malware hosts, C&C servers, and anonymous proxy servers which would allow bypass of filtering or potential harm to your network.
Pornography	displays sexual acts or explicit images	🟩	Securly provide a “Pornography” category which allows administrators to block access and alert on websites that contain pornographic or explicit images and media.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Securly provide a “Streaming Media” category to restrict access to streaming media providers. The “Network Misuse” category will restrict access to common filesharing platforms. Enforced “Creative Commons” mode can be enabled for image search to limit results to only those available under the creative commons license.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Securly uses AI sentiment analysis to detect self-harm content, emails, web searches and social media posts. Securly will flag vulnerable persons activity in real-time to enable emergency intervention.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Securly AI sentiment analysis will detect and flag violent content to Safeguarding contacts in real-time. Websites promoting or hosting graphic violent content, and gore are blocked.

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

- 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 the page content and images.
- Selective HTTPS man-in-the-middle decryption to provide 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.

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

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

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 content and if they need to be filtered.

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

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	🟩	Securly can be configured to define separate filtering policies appropriate to different ages or roles. E.g. Staff, Primary Students, Senior Students.

● 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.	🟩	Securly provide a "Network Misuse" category will prevent access to websites that provide proxy circumvention services or VPN. Securly publish best practice guidance on how to help prevent circumvention. Securly MDM and Classroom can help restrict access to applications and teachers monitor workstations.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	Securly administrators can permit or deny by using their own domain names and keywords globally or per policy.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Securly publishes details of its filtering approach and rationale on the publicly available knowledgebase. More information on Securly Pagescan technology can also be found on our tech blog. https://blog.securly.com/2018/08/10/pagescan-a-deep-dive-into-securlys-url-categorization-technology/
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	As a cloud-based service, the Securly Safety Console is available anywhere with Internet access. Delegated control can be provided to additional administrators or Safeguarding teams. Multiple sites and take-home policies can all be managed from the same central dashboard.
● Identification - the filtering system should have the ability to identify users	🟩	Securly integrates with Microsoft Azure AD, Windows Server Active Directory, and Google G-Suite to provide user identification.
● 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)	🟨	Securly 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. We strongly recommend Securly Filter is combined with mobile device management such as Securly MDM to ensure only appropriate applications can be installed.

● Multiple language support – the ability for the system to manage relevant languages	🟩	Securly implements multiple language support for both filtering and management interface in English, French, and Spanish. Language support is being continually developed and additional languages will be added as available.
● Network level - filtering should be applied at ‘network level’ ie, not reliant on any software on user devices	🟩	As Securely is cloud based it can be implemented at the ‘network level’ using DNS or network settings and does not require software deployed on devices.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Securly automatically reports back content that should be blocked using PageScan. Customers can also make manual submissions via our website. End users also can be provided with a link to submit feedback to administrators.
● Reports – the system offers clear historical information on the websites visited by your users	🟩	Securly has designed reports and alerts to be delegated to school management and safeguarding teams to allow quicker response to incidents. 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. Filters can be applied by user, date/time, category and policy.

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

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

Securly:// 24
A dedicated team of trained student safety coordinators provide 24/7 monitoring of alerts and support to school safeguarding contacts.

The team also provide training sessions, webinars and regularly updated materials available to Schools to help teach pupils and define their own safeguarding policies and best practices.

Securly:// Tipline
Give students, parents, and teachers an open line of anonymous communication to speak up when something feels wrong. When someone submits a tip, a thorough risk assessment is performed. When an alert is determined to be urgent, it follows an escalation process to notify the school. With Tipline, you get the alerts that need your attention.

Securly:// Home
Extend filtering and safeguarding coverage on school devices which go home and help increase parental engagement. Simple management and reporting via our Parent Portal and App.

Securly:// Auditor
Extending Safeguarding beyond the web to protect vulnerable persons while using productivity suites and communication tools, such as Google Gsuite, Gmail and Microsoft Office 365. AI-based real-time notifications of high-risk activity, such as nudity, cyberbullying, suicide, and violence.

Securly:// Classroom
Classroom is a cloud-based classroom management tool, giving teachers new freedom to guide, monitor and communicate with students during class. Remove distractions and keep kids focused on learning.

Securly:// MDM
Securly MDM brings simplified mobile device management to Apple devices. Designed specifically for schools, we've built every feature with your needs in mind. MDM also includes classroom device management tools to keep students on task and maximize every educational moment spent on school devices.

[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	Chris Humby
Position	Securly EMEA Technology Manager
Date	25th June 2020
Signature	Chris Humby