Appropriate Filtering for Education Settings
2026
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"*.

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://securly.com
Contact details	uksales@securly.com 0141 343 8322
Filtering System	Securly Filter and Aware
Date of assessment	2026-06-01

System Rating Response

Where a supplier is 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 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 has been an IWF member since 01/03/2016.
Block access to illegal Child Abuse Images (by actively implementing the IWF URL list), including frequency of URL list update		Securly receives and incorporates the IWF and CTIRU feeds into its filtering technology. Securly blocks access to illegal content including CSAM. Lists are imported at least twice daily.
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).
Confirm that filters for illegal content cannot be disabled, overridden, or altered by any user in a school, college, multi-academy trust (MAT), local authority (LA) or any other responsible body, including system administrators, at any level.		IWF and CTIRU blocklists are implemented at the system level within Securly Filter. These blocklists cannot be disabled, overridden, or altered by any user - including school administrators, MAT-level administrators, or any other responsible body. No user at any level has the ability to remove items from or override these blocklists.

Describing how their system manages the following illegal content:

Content	Explanatory notes	Rating	Explanation
Child sexual abuse	*Content that depicts or promotes sexual abuse or exploitation of children.*		Securly Filter and Securly Aware strictly prohibit and actively block or flag any content that depicts or promotes child sexual abuse or exploitation.
Controlling or coercive behaviour	*Online actions that involve psychological abuse, manipulation, or intimidation to control another individual.*		Securly Aware monitors and flags online behaviour that may indicate psychological abuse, manipulation, or intimidation. The system identifies concerning online activities, such as threatening language or expressions of emotional distress, through monitoring of emails, social media posts, and web searches. Flagged activities related to violence, bullying, or emotional harm are displayed for review by administrators, enabling timely intervention.
Extreme sexual violence	*Content that graphically depicts acts of severe sexual violence.*		Securly Filter blocks and monitors access to websites that contain sexually explicit and adult content, including material depicting extreme sexual violence, in compliance with legal requirements. Attempts to access such content are reported and monitored to support school administrators in maintaining a safe online environment.
Extreme pornography	*Pornographic material portraying acts that threaten a person's life or could result in serious injury.*		Securly Filter blocks and monitors access to pornographic and explicit websites, including material that is obscene, unlawful, or involves acts that threaten a person's life or could result in serious injury. This helps ensure compliance with legal standards and protects users from exposure to extreme pornography.
Fraud	*Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain.*		The Securly Filter "Malware" category actively blocks access to domains associated with fraud, including phishing and scam activities, by leveraging threat intelligence and real-time updates to maintain a secure online environment.

Racially or religiously aggravated public order offences	*Content that incites hatred or violence against individuals based on race or religion.*		The Securly Filter "Hate" category blocks content that incites hatred or violence against individuals or groups based on race or religion, directly addressing concerns about racially or religiously aggravated public order offences.
Inciting violence	*Online material that encourages or glorifies acts of violence.*		Online material that incites or glorifies violence may be blocked under the "Other Adult Content" category in Securly Filter if it is explicit or graphic. Securly Aware also monitors for and flags violent content, alerting school authorities for review.
Illegal immigration and people smuggling	*Content that promotes or facilitates unauthorised entry into a country.*		Content promoting or facilitating illegal immigration and people smuggling is not addressed by a dedicated filtering category. However, such content is likely to be identified and blocked through Securly's multi-layered approach: sites offering illegal services are commonly categorised under existing blocked categories by PageScan's AI-driven classification engine, which analyses page content, metadata, and structure. Where specific sites are identified as promoting illegal activity, administrators can add them to the Global Block List. Securly Aware may also flag related content encountered within school-managed email and collaboration platforms through its sentiment analysis capabilities.
Promoting or facilitating suicide	*Material that encourages or assists individuals in committing suicide.*		Securly Aware is specifically designed to identify and support students at risk of suicide, self-harm, and related distress signals. The platform analyses students' online activities (including emails, documents, web searches, social media, and AI prompts) to detect early warning signs of suicide ideation or material that encourages or assists individuals in committing suicide. When such content is detected, Securly Aware alerts school counsellors and support teams so they can respond quickly and appropriately.

Intimate image abuse	*The non-consensual sharing of private sexual images or videos.*		Securly Aware's nude image quarantine and Securly Filter's in-browser image scanning and blurring feature detect, restrict, and securely manage incidents of intimate image abuse, minimising harm and protecting student privacy.
Selling illegal drugs or weapons	*Online activities involving the advertisement or sale of prohibited substances or firearms.*		Securly Filter provides a dedicated "Drugs" category that blocks access to websites associated with the advertisement or sale of prohibited substances. Weapons-related content is addressed through the "Other Adult Content" category in Securly Filter, which includes most weapons-related terms in its classification. Securly Aware additionally monitors for and flags weapons-related terms across school-managed email, documents, chat platforms, and web searches, alerting designated safeguarding staff for review. Administrators can further supplement category-based filtering by adding specific domains to the Global Block List. Securly's PageScan classification engine analyses and categorises previously unknown sites, including those offering weapons for sale, based on page content analysis.
Sexual exploitation	*Content that involves taking advantage of individuals sexually for personal gain or profit.*		Securly Filter blocks access to websites likely to contain sexual exploitation content through its Pornography, Other Adult Content, and Sexual Content categories.
Terrorism	*Material that promotes, incites, or instructs on terrorist activities.*		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).

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	Rating	Explanation
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.
Hate speech / Discrimination	*Content that expresses hate or encourages violence towards a person or group. Promotes unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.*		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.
Harmful content	*Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.*		Securly addresses harmful content through both filtering and monitoring. Securly Filter's "Other Adult Content" category blocks access to websites containing content not appropriate for educational settings, including graphic, violent, or harmful material depicting or encouraging serious violence or injury. Securly Aware provides AI-driven monitoring for bullying, violence, and harmful behaviour across school-managed email, documents, chat platforms, and web searches, flagging content for review by designated safeguarding staff. Where content encouraging dangerous stunts, challenges, or the ingestion of harmful substances is hosted on sites not yet categorised, Securly's PageScan engine analyses page content in near real-time to apply an appropriate category. Administrators can also block specific sites or search terms through policy-level controls.
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.
Mis / Dis Information	*Promotes or spreads false or misleading information intended to deceive, manipulate, or harm.*		Securly does not maintain a dedicated misinformation or disinformation filtering category. This is a content type that is inherently difficult to address through category-based filtering, as misleading content often appears on otherwise-legitimate news, social media, and reference platforms. Securly's approach is therefore layered: PageScan analyses page text, metadata, images, and structure to classify previously unknown sites, and may categorise content under "Hate" or "Network Misuse" where applicable. Administrators can request reclassification of specific sites and add domains or keywords to the Global Block List on a per-policy basis. Within school-managed collaboration platforms, Securly Aware's sentiment analysis may surface content indicating exposure to or sharing of harmful or misleading material, supporting curriculum-led media literacy work alongside technical controls.
Piracy and copyright theft	*Includes illegal provision of copyrighted material.*		Securly provides a "Streaming Media" category to restrict access to streaming media providers. The "Network Misuse" category restricts 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 licence.
Pornography	*Displays sexual acts or explicit images and text.*		Securly offers a "Pornography" category. This allows administrators to both block access to and receive alerts for websites that contain explicit images or display sexual acts.

Self-Harm and eating disorders	*Content that encourages, promotes, or provides instructions for self-harm, eating disorders or suicide.*		Securly provides a dedicated "Self-Harm/Grief" monitoring feature within Securly Aware, which allows administrators to detect, review, and respond to content that encourages, promotes, or provides instructions for self-harm, eating disorders, or suicide. The system uses advanced sentiment analysis and real-time monitoring of searches, social media, and browser activity to flag and alert on such content, supporting timely intervention and student safety.
Violence Against Women and Girls (VAWG)	*Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls.*		Securly provides a "Violence" monitoring category within Securly Aware, which allows administrators to detect, review, and respond to content that promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls. The system uses advanced sentiment analysis and real-time monitoring of searches, social media, and browser activity to flag and alert on such content, supporting timely intervention and student safety.

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

Audit logs keep a record of each instance when an admin or teacher allows a site.

Securly Filter categories include keywords/phrases, URLs and domains of over 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. PageScan operates in near real-time, typically categorising new sites within seconds. Administrators can submit sites for recategorisation; the majority of these requests are vetted automatically using an LLM, with the remainder reviewed manually.

Selective HTTPS man-in-the-middle decryption provides real-time dynamic URL filtering, keyword filtering and sentiment analysis on inspected categories including search engines, shopping sites, and streaming media platforms.

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, 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 - 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.

Testing filtering effectiveness: schools are increasingly asked to evidence the effectiveness of their filtering provision. SWGfL's testfiltering.com provides a useful baseline confidence check at the network and browser level, and Securly Filter is tested against it regularly. Schools should be aware that testfiltering.com primarily exercises web browser-based access; it does not test app-delivered content, in-app browsers, or app-level traffic. Securly recommends that schools structure their annual filtering checks to cover both browser and app-based access from a managed mobile device, on and off the school network, with and without the browser extension installed, and on any BYOD or unmanaged devices that connect to the school network. Test results should be recorded with the device, location, user, and configuration alongside the outcome. Some tests depend on configuration (managed devices, certificate deployment, managed browsers); the test result reflects the deployment tested, not Securly's full capability.

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 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). 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 retained for 7 days; Logs - monthly backups retained for one month. Data is replicated across geographically separate availability zones.

Securly provides a Data Processing Agreement (DPA) to all UK customers and can support schools in completing Data Protection Impact Assessments (DPIAs) as recommended by the ICO. Securly's data residency for UK customers is AWS EU-West-2 (London).

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 selectively intercepts web traffic to block and filter content. This prevents over-blocking or problems accessing safe content and education applications.

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

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

Securly provides a mechanism for staff and students to request access to blocked sites directly from the block page, as well as a manual submission process via our website.

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		Securly Filter is built exclusively for education and has school-appropriate filtering configured out-of-the-box, allowing easy configuration of more strict or relaxed policies as required. Securly 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. Securly 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.
Circumvention - the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services, DNS over HTTPS and ECH.		Securly works with schools to ensure Securly 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. Securly provides a "Network Misuse" category to prevent access to websites that provide proxy circumvention services or VPNs. Securly publishes best practice guidance on how to help prevent circumvention. Securly MDM and Classroom can help restrict access to applications, and allows teachers to monitor student devices.
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 ensures transparency and that individuals are not able to make unilateral changes.		Securly administrators can permit or deny access to content by using their own domain names and keywords globally or per policy. 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. Any substantial changes to the system are logged in an audit trail.

Contextual Content Filters - the ability to analyse online content based on its meaning and context, rather than relying solely on website categories or domain lists. Systems should be capable of identifying harmful or inappropriate content within otherwise permitted platforms, including dynamically generated webpage content. Schools should understand how their filtering system analyses encrypted connections and whether contextual inspection takes place on decrypted content.		Securly Filter provides contextual content analysis through multiple complementary mechanisms, with the depth of analysis varying by deployment method. Extension (Chrome/Edge on ChromeOS, Windows, macOS): The Securly browser extension uses cross-platform Chrome and Edge APIs to inspect page content at the DOM level directly on the device, without requiring man-in-the-middle (MITM) decryption. This enables real-time contextual analysis of dynamically generated content within otherwise permitted platforms - including the ability to detect proxy and gaming content embedded within allowed sites, and to monitor and apply policy-based guardrails to student prompts submitted to third-party Generative AI tools such as ChatGPT and Google Gemini. The extension also provides on-device image scanning, detecting and blurring nudity in images displayed within the browser in real-time; this is configurable by school administrators. Because the extension operates within the browser itself, it is not limited by TLS encryption in the way that network-level inspection would be. SmartPAC and SmartDNS: These methods apply selective MITM decryption to traffic destined for domains within blocked or inspected categories - primarily search engines, but also including shopping sites (e.g. Amazon) and streaming media platforms (e.g. YouTube) - enabling keyword and search term filtering on those sites. Where a domain is categorised as allowed and is not in an inspected category, traffic from that site passes without content-level inspection. This approach minimises latency and avoids over-blocking, while still providing search term and keyword analysis where it is most relevant. SmartPAC and SmartDNS can also block access to Generative AI platforms at the domain level and, where configured, redirect users to Securly AI Chat - a controlled environment with built-in safety guardrails. YouTube restrictions and search term inspection are supported across all filtering methods. PageScan (all methods): Securly's backend classification engine, PageScan, analyses the content of previously uncategorised websites using AI and human moderation. While not inline, PageScan operates in near real-time, typically categorising new sites within seconds. All filtering methods feed into PageScan. Administrators can also submit sites for recategorisation; the majority of these

		requests are vetted automatically using an LLM, with the remainder reviewed manually. Securly Aware: Operating independently of the filtering method deployed, Securly Aware connects via API to Google Workspace and Microsoft 365 to scan emails, documents, chat messages, and files for harmful content - including cyberbullying, self-harm, violence, and nudity - using AI-driven sentiment analysis and image recognition. This provides contextual monitoring of collaboration platforms regardless of device, operating system, or network. Transparency on limitations: The extension provides the deepest level of contextual analysis, including inspection of dynamically generated content, but is limited to Chrome and Edge browsers. SmartPAC and DNS methods do not perform content-level analysis on allowed domains. Apps or services that use certificate pinning, non-HTTP/HTTPS protocols, or end-to-end encryption may not be subject to contextual filtering at the network level. Schools deploying DNS-only or Guest DNS filtering will receive domain-level blocking without keyword or content inspection. For the fullest contextual filtering coverage, Securly recommends deploying the browser extension on managed devices alongside SmartPAC or DNS filtering.

Deployment - filtering systems can be deployed in a variety (and combination) of ways. Providers should describe how their systems are deployed alongside any required configurations and/or limitations.		Securly Filter offers several deployment options for educational settings: Extension - Provides real-time, customised filtering and monitoring within the Chrome and Edge browsers on student devices, regardless of location. Supports ChromeOS, Windows, and macOS. SmartPAC - A cloud-based proxy auto-configuration solution that integrates with school networks and MDM solutions to analyse web traffic and enforce filtering. Supports Windows, macOS, and iOS/iPadOS. Requires the Securly SSL certificate. SmartDNS - Network-level protection that blocks harmful websites before they load, effective for all connected devices without needing per-device software. Requires SSL certificate for MITM inspection. Guest DNS - Ensures visitors on the school network adhere to filtering policies without requiring certificates or device management. These methods can be combined for a tailored filtering solution. Securly recommends combining network-level filtering with device-level configurations tailored to school-owned and managed devices.
Filtering Policy - the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as how the system addresses 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.
Group / Multi-site Management - the ability for deployment of central policy and central oversight or dashboard.		As a cloud-based service, Securly Filter and Aware are 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. 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.

		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.
Identification - the filtering system should have the ability to identify users and devices to attribute access and allow the application of appropriate configurations and restrictions for individual users.		Securly Filter can be applied to managed browsers and managed devices, with user-level logging and filtering through sign-in with Microsoft Azure/Entra ID or Google Workspace. Securly integrates with Microsoft Azure AD/Entra ID, Windows Server Active Directory, and Google Workspace to provide user identification. Activity reports contain detailed information about the activity selected for specific users or OUs, including: the student and OU/Group names, type of activities, policies applied, categories, whether activity has been Allowed, Blocked or Flagged, and the date and time stamp of each event.

Mobile and App content - Filtering should apply to content accessed through mobile devices and applications. Schools should understand what filtering is technically possible across different device types and operating systems, and any limitations that apply.		Securly Filter supports filtering on mobile devices and within applications through a combination of deployment methods, with the extent of coverage depending on the platform, device management approach, and configuration in place. ChromeOS (Chromebooks): The Securly browser extension provides comprehensive filtering coverage for all web activity within the Chrome browser, including DOM-level content inspection, GenAI guardrails, image scanning, and full YouTube controls. ChromeOS devices managed via Google Workspace Admin Console receive the deepest level of filtering and monitoring available. Android apps running on ChromeOS are subject to DNS or network-level filtering policies where SmartDNS is also deployed, but are not inspected at the content level by the browser extension. iOS/iPadOS (iPads and iPhones): Securly Filter is deployed on iOS devices via SmartPAC, configured as a Global HTTP Proxy through a Mobile Device Management (MDM) solution such as Jamf, Mosyle, Meraki, or Intune. This routes all HTTP/HTTPS traffic - including traffic originating from apps, not just the Safari browser - through Securly's filtering infrastructure. Selective MITM decryption is applied to inspected categories (search engines, shopping, and streaming platforms), enabling keyword filtering on those sites. Domain-level blocking applies across all app traffic. The Securly SSL certificate must be deployed alongside SmartPAC for HTTPS filtering to function. SmartDNS can also be deployed on iOS as a complementary or standalone method, providing domain-level filtering across all device traffic. Where apps use certificate pinning, non-HTTP/HTTPS protocols, or end-to-end encryption, filtering may not be able to intervene at the content level. Similarly, app functionality that relies on user-granted permissions - such as access to cameras, microphones, photo libraries, or cloud storage - may operate through device-side or cloud-side processing that is outside the scope of network-level filtering. For this reason, Securly strongly recommends that schools combine Securly Filter with robust MDM controls on managed iOS devices, including restricting which apps can be installed and managing app permissions centrally. For BYOD environments, Securly recommends strict firewall policies, potentially backed by Layer 7/DPI capability, alongside DNS filtering.

		Windows and macOS: The browser extension (Chrome/Edge) provides the fullest filtering capability on these platforms, including DOM-level content inspection and GenAI guardrails. SmartPAC can be deployed alongside or as an alternative, providing HTTP/HTTPS filtering with selective MITM across all browsers. App traffic that uses HTTP/HTTPS is subject to SmartPAC filtering; traffic using non-standard protocols may bypass filtering. Android: Securly supports filtering on Android devices managed via MDM, using SmartPAC or DNS filtering methods. Domain-level blocking and search term filtering (via selective MITM with SmartPAC) apply to HTTP/HTTPS traffic from apps and browsers. As with iOS, apps using certificate pinning or non-standard protocols may not be subject to filtering. Securly Aware (all platforms): Securly Aware operates independently of the device and filtering method. By connecting via API to Google Workspace and Microsoft 365, Aware scans emails, documents, chat messages (Google Chat, Microsoft Teams), and cloud-stored files for harmful content, including nudity detection in images. This provides monitoring coverage for content created, shared, or stored within school-managed collaboration platforms regardless of the device, app, or operating system used. Securly is transparent that no single filtering method can guarantee complete coverage of all app-delivered content across all platforms. The combination of browser extension, SmartPAC, DNS filtering, MDM controls, and Securly Aware provides layered protection, and schools should assess their device estate and deployment configuration to ensure appropriate coverage is in place.
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.
Remote devices - the ability for school owned devices to receive the same or equivalent filtering to that provided in school.		Securly Filter can be applied to school-owned devices regardless of how they access the internet or whether they are within the school network.

		Securly Filter can also be applied to BYOD schemes and Guest networks, ensuring all devices using the school broadband connection are appropriately filtered.
Reporting mechanism - the ability to report inappropriate content for access or blocking.		The Securly block page can be configured to allow staff or students to request sites from the admin. Customers can also make manual submissions via our website. End users can also be provided with a link to submit feedback to administrators.
Reports - the system offers clear granular historical information on the websites users have accessed or attempted to access.		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.
Safe Search - the ability to enforce 'safe search' when using search engines.		Safe Search is supported across all Securly Filter deployment methods (Extension, SmartPAC, SmartDNS) and is applied on a per-policy basis, allowing schools to enforce stricter settings for younger pupils and more relaxed settings for staff or senior students. Securly enforces Safe Search on Google, Bing, DuckDuckGo, and Yahoo by appending the relevant Safe Search parameter to outbound search queries; users cannot disable Safe Search through search engine settings while the policy is active. YouTube is handled separately: schools can apply YouTube Restricted Mode across all deployment methods, and with the browser extension deployed, Securly's YouTube Smart Controls provide more granular control including category-based restrictions, search term filtering, and the ability to whitelist or blacklist specific channels. Image search filtering follows the same model. Schools deploying DNS-only filtering will have Safe Search applied at the DNS resolution level for supported engines; the browser extension and SmartPAC offer the fullest control.

Safeguarding case management integration - the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity.		Securly Filter and Securly Aware natively offer safeguarding case management and can export those details to CPOMS. This integration enhances the understanding of student activities in context, which is crucial for identifying and addressing potential risks. The real-time monitoring capabilities of Securly Aware enable educators to observe student behaviour as it happens, facilitating timely interventions. Additionally, detailed reporting features provide insights into browsing habits and application usage, allowing schools to analyse trends and adapt their safeguarding strategies accordingly.

Generative AI Technologies

How does your filtering system manage access to Generative AI technologies?

Our system manages Generative AI through a hybrid approach of standard URL filtering, redirection, and deep content inspection via browser extensions:

Domain-Level Blocking & Redirection: Securly Filter can identify and block access to Generative AI domains (e.g., chatgpt.com). Administrators can configure a "Redirect" policy that automatically reroutes attempts to access these third-party tools to Securly AI Chat, a safe, walled-garden environment where monitoring and guardrails are enforced natively. This redirect capability is available across all filtering methods including SmartPAC and DNS.

Deep Inspection of Third-Party Tools: For schools that choose to allow access to external tools (e.g., ChatGPT, Gemini, Google Docs with Gemini, Magic School AI), the Securly Filter Extension sits within the browser to inspect and categorise user prompts in real-time. This allows the system to identify prohibited topics (e.g., Drugs, Violence) within the conversation itself, rather than just blocking the website URL.

Access Control (Age, Risk, and Educational Need) - Access and behaviour are controlled using granular, identity-based policies: Organisational Units (OUs) or Security Groups allow schools to apply different restrictions based on age or role (e.g., a "Sixth Form" policy vs. a "Key Stage 3" policy). Through Securly Sync, the system imports student grade levels to automatically tune the AI model's responses, ensuring younger students receive simpler, age-appropriate explanations while older students receive more complex, Socratic guidance. Admins can configure specific topics to be allowed or deflected, and Custom Policies allow schools to input specific text instructions to align with curriculum needs.

Limitations in Filtering AI-Generated Content: When students use external platforms via the extension, the system can analyse and block the student's prompt (input) before it is sent. However, it cannot surgically redact or modify the response (output) generated by the external third-party AI. If a prompt violates policy, the extension blocks the interaction entirely. Monitoring of external GenAI tools and embedded AI requires the Securly Filter Chrome/Edge Extension to be deployed; it is not currently supported via SmartPAC or DNS-only filtering methods. SmartPAC and DNS can block GenAI domains and redirect to Securly AI Chat, but cannot inspect prompts within third-party tools.

Support and Alignment with Safeguarding Frameworks: AI Safety Alerts integrate AI usage with Securly Aware, which scans prompts for indications of risk (self-harm, suicide, bullying, violence), ensuring that AI interactions are monitored for safeguarding risks just like web searches or emails. A dedicated transparency dashboard offers DSLs and IT leads visibility into AI adoption, deflected topics, and high-risk users, enabling schools to audit their provision.

Securly's approach to Generative AI safety in schools aligns with the expectations set out in the DfE's Generative AI: Product Safety Expectations, including risk assessment, content moderation, transparency, and reporting capabilities.

Supporting Teaching and Learning

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

Securly's filtering policies are customisable and policy changes can be applied to specific user groups by the administrator, so that over-blocking does not occur for certain student groups if they are researching legitimate areas to do with sexual health due to the requirements of the RSHE 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 responsible 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 automatically presents 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 provides student safety and wellness monitoring with unprecedented visibility into students' mental health and wellness. On-Call enlists a team of expert analysts to manage Aware alerts and notify schools if a student needs help. Securly Home gives parents control over their child's school device when it goes home. Classroom provides classroom management across Chrome, Windows, and Mac. MDM provides 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	Craig Fearnsides
Position	Senior Director, Product Management
Date	2026-06-01
Signature