Appropriate Monitoring for Schools
2026
Monitoring 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 monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions. The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

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
Monitoring System	Securly Filter, Aware and On-Call
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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
Are IWF members		Securly has been an IWF member since 01/03/2016.
Utilisation of IWF URL list for the attempted access of known child abuse images		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.
Work with CTIRU '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 monitoring 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. Monitoring of illegal content categories within Securly Aware is similarly locked at a system level.

Illegal Online Content

Monitoring providers should both confirm, and describe how, their system monitors/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. 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.
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. Securly Aware monitors for hateful or discriminatory language across school-managed platforms.
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. Securly Aware monitors for and flags violent content across emails, documents, chat platforms, and web searches, 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 or monitoring category. However, such content is likely to be identified through Securly's multi-layered approach: sites offering illegal services are commonly categorised under existing blocked categories by PageScan's AI-driven classification engine. 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. With On-Call enabled, extreme-risk alerts are escalated to trained safety analysts who can

			notify emergency contacts or law enforcement within minutes.
Intimate image abuse	*The non-consensual sharing of private sexual images or videos.*		Securly Aware's nude image quarantine detects and securely manages inappropriate images shared via email and cloud storage. Securly Filter's in-browser image scanning and blurring feature detects and blurs nudity in images displayed within the browser in real-time, configurable by school administrators. Together these capabilities detect, restrict, and 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.
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. Securly Aware monitors for related content across school-managed platforms.
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

Monitoring providers should both confirm, and describe how, their system monitors/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.*		Securly addresses harmful content through both filtering and monitoring. Securly Filter's "Other Adult Content" category blocks access to websites containing graphic, violent, or harmful material. 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.
Malware / Hacking	*Promotes the compromising of systems including anonymous browsing and filter bypass tools.*		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.

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. Attempts to access these categories are logged and can generate alerts for administrator review.
Pornography	*Displays sexual acts or explicit images and text.*		Securly offers a "Pornography" category allowing administrators to both block access to and receive alerts for websites that contain explicit images or display sexual acts. Securly Aware's nudity detection scans images in emails and cloud storage for explicit content.

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.

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 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 requests are vetted automatically using an LLM, with the remainder reviewed manually.

Selective HTTPS man-in-the-middle decryption provides real-time 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 Aware connects via API to Google Workspace and Microsoft 365, scanning emails, documents, chat messages (Google Chat, Microsoft Teams), and cloud-stored files for harmful content using AI-driven sentiment analysis, keyword matching, and image recognition. This monitoring operates independently of the filtering method deployed and regardless of device, app, or operating system.

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

Testing monitoring effectiveness: schools should structure their annual monitoring checks to include both browser-delivered content and content created or shared inside school-managed apps (Google Docs, Microsoft Teams, Outlook, and equivalents) on managed mobile devices, on and off the school network. Browser-based tests will exercise the extension's inspection and alerting; tests inside Google Workspace or Microsoft 365 will exercise Aware's API-based monitoring; the two are independent and should be tested separately. Test results should be recorded with the device, location, user, app, and configuration alongside the outcome. Some tests depend on configuration (managed devices, managed accounts, browser extension installed, MDM-enrolled iOS); the test result reflects the deployment tested, not Aware's full capability.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
Age appropriate - includes the ability to implement variable monitoring appropriate to age and vulnerability. This will in turn define which alerts are prioritised and responded to.		Securly Aware and On-Call enable age-appropriate and vulnerability-sensitive monitoring by allowing policy customisation, flexible alert prioritisation, and scalable human oversight. Monitoring policies can be configured per Organisational Unit or Security Group, enabling different alert thresholds and response workflows for different age groups, roles, or vulnerability levels. This ensures that monitoring and response can be tailored to the needs of different student groups and environments, such as boarding schools or community-based access.
Alert Management - how alerts are managed - if schools manage system alerts or support/management is provided.		Securly's monitoring system allows schools to either manage alerts themselves using Securly Aware's built-in case management tools, or to delegate alert management to Securly's On-Call service for professional, 24/7 support. With Aware alone (Active Monitoring): Alerts are generated by AI analysis and presented to designated school staff via the Aware dashboard, email notifications, and optional SMS. Schools configure alert types, recipients, and hours of operation. With On-Call (Proactive Monitoring): Securly's trained safety analysts review flagged alerts, conduct a thorough risk assessment examining patterns across the student's search history and online activity, and assign a risk level (Moderate, Increased, or Extreme). Schools are notified by email, SMS, and/or phone depending on severity. In extreme-risk cases, designated school personnel are notified within an average of 5 minutes. If contacts are unreachable, law enforcement can be alerted where the school has opted into this.
Audit - Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.		A central "Admin Audit Log" in the Securly portal records all end-user changes made in the web console (e.g., editing an Aware wellness-monitoring policy, adjusting alert-delivery rules, changing user roles, closing or reopening a case). Each entry is time-stamped and records: product (Aware, Filter, etc.), user email, action taken, and the object affected.

BYOD (Bring Your Own Device) - if adopted by the school and the system includes the capability to monitor personal mobile and app technologies, how is this deployed and how data is managed. Does it monitor beyond school hours and location?		Schools can allow BYOD devices to connect to the school's network. IT admins should segment the BYOD network from the main school network for security. Filtering policies for BYOD can match school-owned devices or use a more basic Guest Network Policy. BYOD devices are filtered and their internet activity is logged in the same way as school devices when on the school network. Deployment options include: splash page on the wireless network directing users to download the Securly certificate; instructions posted on the school website or sent via email; manual certificate installation by IT admins. Devices without the certificate are still filtered at the DNS level but HTTPS sites may show SSL errors. Securly Aware's API-based monitoring of Google Workspace and Microsoft 365 applies regardless of device ownership, location, or network - if the student is using their school-managed account, monitoring applies whether they are on a school device or a personal device, on or off campus.
Data retention - what data is stored, where is it stored and for how long. This should also include any data backup provision.		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. 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).

Devices - if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers.		The Securly Extension (Chrome/Edge) provides the deepest monitoring capability on ChromeOS, Windows, and macOS devices, including DOM-level content inspection, GenAI prompt monitoring, and in-browser image scanning. SmartPAC provides HTTP/HTTPS monitoring with selective MITM decryption on Windows, macOS, and iOS/iPadOS devices. SmartDNS and Guest DNS provide domain-level monitoring for all device types including unmanaged devices. Securly Aware operates independently of device type or filtering method, connecting via API to Google Workspace and Microsoft 365 to monitor emails, documents, chat messages, and cloud-stored files regardless of the device or operating system used. For unmanaged devices, SmartDNS and Guest Network Policy ensure that all traffic originating from the school network is subject to filtering without requiring software installation.
Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy.		Securly's filtering and monitoring policies are customisable and changes can be applied to specific user groups by the administrator. This ensures that over-blocking or over-monitoring does not occur for student groups researching legitimate areas - for example, sexual health content required by the RSHE and PSHE curriculum. Administrators can add custom keywords in any language to their local blocklists, allowing schools to tailor monitoring to their specific community demographics.
Group / Multi-site Management - the ability for deployment of central policy and central oversight or dashboard.		As a cloud-based service, Securly Filter, Aware, and On-Call 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 monitoring 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 logged in the Audit log for that specific school.

Harmful Image detection - The inclusion or extent to which visual content is discovered, monitored and analysed.		Securly Aware's nude image quarantine detects and securely manages inappropriate images shared via email (Gmail, Outlook) and cloud storage (Google Drive, OneDrive). Securly's AI engines can identify and flag almost all types of nude images irrespective of skin colour or image size. To keep false positives at bay, nudity in sculptures, certain paintings, and other works of art is not flagged. Securly Aware automatically recalls emails containing violence, bullying, or nudity. Securly Filter's in-browser image scanning and blurring feature, available via the browser extension, detects and blurs nudity in images displayed within the browser in real-time. This is configurable by school administrators. Google Drive files, OneDrive files, emails, social media, and web searches are scanned to identify indications of suicide, depression, violence, bullying, and nudity.
Identification - the monitoring system should identify users and devices to attribute activity and ensure the application of appropriate configurations 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 syncs directly with the school's directory services (Google Workspace or Azure AD). This "Dual Provisioning" capability supports mixed-mode environments. When a user logs into a device, the Securly extension reads the user identity token, ensuring that the policy follows the user, not the hardware. Activity reports contain detailed information for specific users or OUs/Security Groups, including student name, OU/Security Group, policy applied, and time-stamped events. For BYOD devices using SmartDNS, user identification can be achieved via a Captive Portal or Splash Page where the user authenticates to associate their session with their username.

Impact - How do monitoring results inform your policy and practice?		Securly Aware creates a Student Wellness Level for every monitored user, calculated from a 60-day rolling window of flagged activity. This provides school leadership and DSLs with a longitudinal view of student wellbeing trends, enabling data-informed decisions about safeguarding policy and practice. Securly offers a Filtering and Monitoring Annual Review service that includes: strategic reviews of filtering and monitoring policies; review of adequate filtering and monitoring procedures; and data assessment and insights covering activity, alerts, and safeguarding trends. These reviews help schools evidence their filtering and monitoring effectiveness as required by the DfE's Filtering and Monitoring Standards. Reporting dashboards provide visibility into which categories are most frequently triggered, which student groups are most at risk, and how alerts are being resolved - enabling schools to refine their monitoring strategy iteratively.
Monitoring Policy - How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		We recommend schools allow for monitoring within their own Acceptable Usage Policy (AUP) and IT policies so all users are aware. Securly can assist by providing templates and training webinars on what should be included. Deployment options for BYOD include a splash page on the wireless network directing users to download the Securly certificate, which serves as a point of notification. While the technical enforcement is handled by the software, Securly places the onus of policy communication on the school while providing the tools to facilitate it.

Mobile and app content - Mobile and app content is often delivered through different mechanisms from that delivered through a traditional web browser, including embedded browsers within apps and in-app link handling. Schools should understand to what extent the monitoring system operates across mobile devices and app content, including whether it can inspect or report on activity occurring within apps.		Securly's monitoring of mobile and app content operates through two complementary approaches: browser-level monitoring and API-based platform monitoring. Browser-level monitoring (Extension): On ChromeOS, Windows, and macOS, the Securly browser extension monitors all web activity within Chrome and Edge browsers, including content accessed via web-based apps and embedded web views. This includes DOM-level content inspection, GenAI prompt monitoring, and in-browser image scanning. API-based platform monitoring (Aware): Securly Aware connects server-to-server with Google Workspace and Microsoft 365 via API, scanning emails, documents, chat messages (Google Chat, Microsoft Teams), and cloud-stored files for harmful content. This monitoring operates regardless of the device type, app, or operating system used. If a student writes concerning content in a Google Doc using the Google Docs app on an iPad at home, Securly Aware detects it because it scans the file, not the network traffic. Transparency on limitations: Many mobile apps (e.g. WhatsApp, Snapchat, Instagram) use certificate pinning, which prevents third-party inspection of traffic. App functionality that relies on user-granted permissions, such as access to cameras, microphones, photo libraries, or third-party cloud storage, may operate through device-side or cloud-side processing that is outside the scope of network-level monitoring. Where the destination is a school-managed platform (Google Workspace, Microsoft 365), Aware's API-based monitoring will detect harmful content once it lands in school systems. Where content remains entirely within a third-party app or its associated cloud, for example a personal Snapchat account or a non-school iCloud library, monitoring at the network or API level is not technically feasible. Schools should combine Securly monitoring with MDM controls over app installation, app permissions, and managed accounts to constrain where pupil activity can take place. Deep content inspection inside a proprietary app is therefore not technically feasible via web filtering alone. Securly addresses this for the most critical school platforms through API-based scanning via Aware. For other apps, schools should combine Securly monitoring with robust MDM

		controls to restrict which apps can be installed on managed devices. On iOS/iPadOS, SmartPAC deployed via MDM as a Global HTTP Proxy routes all HTTP/HTTPS traffic through Securly's infrastructure, providing domain-level monitoring and selective MITM inspection on inspected categories. Aware's API-based monitoring covers Google and Microsoft platform activity regardless of device. On Android, SmartPAC or DNS filtering provides domain-level monitoring. Aware's API-based monitoring applies as on all other platforms.
Multiple language support - the ability for the system to manage relevant languages.		Securly implements multiple language support for both filtering and the management interface in English, French, and Spanish. Language support is being continually developed and additional languages will be added as available. Administrators can add custom keywords in any language to their local blocklists, allowing schools to tailor monitoring to their specific community demographics.

Prioritisation - How are alerts generated and prioritised to enable a rapid response to immediate issues?		Securly Aware creates a Student Wellness Level for every monitored user, calculated from a 60-day rolling window of flagged activity. Multiple flagged activities decrease the wellness score over time. Certain “mayday” phrases or high-severity triggers can immediately elevate a student to Critical status. The Aware AI engine uses natural language processing (NLP), sentiment analysis, and keyword analysis to determine the severity of an activity and update wellness levels. Based on this analysis, real-time alerts are created and cases are generated, enabling designated staff to monitor all notifications within their assigned OUs. SLT or DSLs can quickly identify students who are trending negatively, drill down into individual wellness levels, and gain insight into contributing online activities. With On-Call enabled, Securly’s trained safety analysts review flagged alerts, prioritise based on wellness level, and conduct a thorough risk assessment examining patterns across the student’s online activity. Alerts are assigned a risk level of Moderate, Increased, or Extreme. In extreme-risk cases, designated school personnel are notified within an average of 5 minutes. If contacts are unreachable, law enforcement can be alerted where the school has opted into this.

Remote monitoring - the ability, extent and management for the monitoring of devices. Monitoring should focus on school-owned and managed devices. When shared devices are used, schools should ensure users log in individually.		Securly Filter can be applied to school-owned devices regardless of how they access the internet or whether they are within the school network. The policies applied on-site (via extension or SmartPAC) persist when the device goes home. Securly Aware's API-based monitoring of Google Workspace and Microsoft 365 applies to school-managed accounts regardless of location or device. This ensures continuous monitoring of collaboration platforms whether the student is at school, at home, or elsewhere. Securly Home is a free feature included with the 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. When shared devices are used, Securly's user-identity-based approach ensures that monitoring follows the user, not the hardware. A Year 7 student logging into a library computer receives Year 7 monitoring, while a teacher logging into the same machine receives staff-level monitoring.
Reporting - how alerts are recorded, communicated and escalated.		Securly offers robust, user-friendly reporting that includes prebuilt reports for common use cases and custom report creation by activity type, user, OU/Security Group, or date range. A central "Admin Audit Log" records all changes to the system, timestamped with the user email and action taken. Reports make visually clear which sites are accessed or blocked. Filters can be applied by user, date/time, category, and policy. With On-Call, escalation follows a formal protocol: Moderate and Increased risk alerts generate email and optional SMS notifications; Extreme risk alerts trigger direct phone calls from On-Call analysts to designated contacts, with multiple contact attempts via SMS and phone. Schools can customise their escalation plan, including specifying which contacts are reached at which times and for which risk levels.

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. For schools without external systems, Securly Aware provides a built-in Case Management interface where alerts can be assigned to staff, annotated with notes, and marked as resolved. The real-time monitoring capabilities of Securly Aware enable educators to observe student behaviour as it happens, facilitating timely interventions. Detailed reporting features provide insights into browsing habits and application usage, allowing schools to analyse trends and adapt their safeguarding strategies accordingly.

Proactive Monitoring

How any proactive monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams:

Securly offers institutions a range of preventative tools to support student safeguarding and wellness.

Securly Aware creates a Student Wellness Level for every monitored user, calculated from a 60-day rolling window of flagged activity. SLT or DSLs can quickly identify students who are trending negatively, drill down into individual wellness levels, and gain insight into contributing online activities. This enables proactive investigation and preventative support before students become extreme risks.

Use of automation: Securly's Aware AI engine uses natural language processing (NLP), sentiment analysis, and keyword analysis as the first line of defence to determine the severity of an activity and update wellness levels. This AI-driven triage processes the volume of student activity and surfaces the most relevant alerts for human review. Certain high-severity triggers ("mayday" phrases, such as searches for suicide hotlines or instructions on planning self-harm) can immediately elevate a student to Critical status and alert the On-Call team. For one-off alerts that are not escalated to On-Call, the activity is still flagged and visible to school staff via the Aware dashboard and to parents via the Securly Home app.

On-Call service: Schools can enlist Securly's On-Call team of trained safety analysts to manage Aware alerts 24/7. Every flagged alert reviewed by On-Call receives a thorough human risk assessment examining patterns across the student's search history and online footprint. Analysts assign a risk level of Moderate, Increased, or Extreme. In extreme-risk cases, designated school personnel are notified within an average of 5 minutes via email, SMS, and phone. If contacts are unreachable, law enforcement can be alerted where the school has opted into this. Schools can customise their escalation plan, including specifying contacts for particular categories, risk levels, and times of day.

Securly Aware's 'Think Twice' cyberbullying prevention widget promotes responsible digital citizenship by prompting 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.

Recall and quarantine: Securly Aware automatically recalls emails containing violence, bullying, or nudity, and quarantines inappropriate images for administrator review.

Roles, interpretation, and limitations: monitoring alerts are technical signals, not safeguarding decisions. Securly Aware uses AI-driven sentiment analysis, keyword matching, and image recognition to surface activity that may warrant attention; interpretation of those signals, assessment of context, and any safeguarding response sit with the school's Designated Safeguarding Lead and wider safeguarding team. The system is designed on the assumption that IT or technical staff administer the platform but do not hold safeguarding decision-making responsibility. Securly is explicit with schools that monitoring systems produce false positives by design; sentiment analysis cannot reliably distinguish a creative writing exercise about violence from a genuine threat, and image recognition will occasionally surface benign content. Human review, by school staff or, with On-Call, by trained Securly safety analysts, is integral to the model. Monitoring should be used proportionately, alongside the school's acceptable use policy, curriculum-based online safety education, and pastoral practice.

Please note below opportunities or enhancements to support schools with their obligations around Keeping Children Safe in Education:

Securly is a student safety company and provides services beyond web filtering and student wellness monitoring.

On-Call - Enlist a team of expert analysts to manage your school's Aware alerts and notify you if a student needs help now. The service operates 24/7 and follows a formal escalation protocol.

Training sessions and material provided to schools to help follow best practice and integrate Securly technology into their safeguarding procedures.

Securly Filtering and Monitoring Annual Review: strategic reviews of filtering and monitoring policies; review of adequate filtering and monitoring procedures; data assessment and insights covering activity, alerts, and safeguarding trends.

Securly Home - Parent app 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.

Generative AI Technologies

How does your monitoring system identify and respond to activity involving Generative AI technologies?

Our system monitors 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 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 within the conversation itself, and all AI interactions are logged and can generate safeguarding alerts via Securly Aware.

Access Control: AI policies inherit the user directory and mapping from Securly Filter, allowing schools to apply different restrictions based on age or role. Through Securly Sync, the system imports student grade levels to automatically tune AI model responses. 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: When students use external platforms via the extension, the system can analyse and block the student’s prompt before it is sent. However, it cannot modify the response generated by the external third-party AI. Monitoring of external GenAI tools requires the Securly Filter Chrome/Edge Extension; it is not currently supported via SmartPAC or DNS-only methods. SmartPAC and DNS can block GenAI domains and redirect to Securly AI Chat, but cannot inspect prompts within third-party tools.

AI Safety Alerts: AI usage is integrated with Securly Aware, which scans prompts for indications of risk (self-harm, suicide, bullying, violence), ensuring 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.

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.

Monitoring 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