Appropriate Monitoring for Schools

May 2025

Monitoring Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help 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	**Securus Software Ltd**
Address	Freedom Works, Fairmount House, Bull Hill, Leatherhead, KT22 7AH
Contact details	Bernard Snowe (CEO) - Bernard.snowe@securus-software.com Tel: 0330 124 1750
Monitoring System	Securus XT for Windows Securus XT for Chrome Securus Safeguard Browser for iPads Securus NET for BYOD & Personal Devices ALL THE ABOVE TECHNOLOGY HAS 2 MONITORING OPTIONS: Securus Full Monitoring Solution (FMS) or Securus Self-Managed Monitoring Solution
Date of assessment	5 June 2026

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.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		Yes, as members of the IWF, Securus integrates the IWF keyword list into our own safeguarding library of words and phrases. These lists are frequently reviewed by our internal library team.
• Utilisation of IWF URL list for the attempted access of known child abuse images		Not currently, as a supplier of monitoring solutions, we utilise the IWF Keywords List, however we do not currently offer a filtering solution and therefore we do not use the IWF URL List
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, we work with the CTIRU to monitor attempted access to their list of unlawful terrorist content. This includes deliberate searches as well as content users may inadvertently encounter.
• Confirm that monitoring for illegal content cannot be disabled by anyone (including any system administrator) at the school		Multiple preventative designs to ensure that the monitoring of illegal content is maintained. This includes tamper proofing and hidden library elements. The software will log the user out of the computer should they manage to force stop the application process. This ensures continuity of monitoring on school managed devices.

Illegal Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.		We have many words, phrases and acronyms to support the monitoring of CSAM and SA activity. The software and service models allow images to be password protected / blurred from visibility. We also have a strict protocol in place should CSAM be encountered.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another		We monitor controlling and coercive behaviour across several of the library categories. Said

	individual, often occurring in domestic contexts.		terms range from monitor to urgent in nature.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.		Sexual violence is covered by multiple categories including pornography, violence, shock content. In cases where schools / organisation or our team of moderators encounter ESV activity this will be raised with the appropriate authorities.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.		Monitored by way of relevant library terms as well as websites known to contain extreme pornographic content.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		Whilst we do not offer a dedicated category for the purposes of monitoring fraud, many words and phrases in our library cover malicious and harmful intent, plus organisations can add their own custom terms to the monitoring library.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.		Securus has a highly developed category dedicated to monitoring racism generally. This includes content inciting hatred, collusion and possible coordination of public disorder.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.		Specific monitoring to violent intent, arrangements to harm. All on screen activity including forums are compared with library terms.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.		Whilst we do not offer a dedicated category for the purposes of monitoring illegal immigration and people smuggling, unusual behaviour from high risk individuals would potentially trigger captures plus organisations can add their own custom terms to the monitoring library.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.		Suicide, mental health and self-harm are standard categories within Securus. Most of these terms are marked by default with the highest severity score.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		Terms relevant to the distributing or sharing of sensitive images are updated within our library. This includes the likely language encountered in the use and sharing of intimate image abuse between individuals.

selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.		One of our dedicated categories is drugs. This includes drug names / slang terms. Frequently reviewed to ensure ever changing drug slang is accommodated. This is also true for weapons including firearms, knives & blunt weapons. Many phrases used around buying, selling, finding weapons are kept up to date within the global library.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		We cater for this topic across multiple categories. One of these categories 'Grooming' contains words around exploitation and incentivisation.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		Radicalisation, including content classed as Extremism in nature, is a standard category. Guidance and courses around PREVENT are utilised within our definitions.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Gambling	Enables gambling		Dedicated category for gambling where age restriction applies. Betting sites are added to this category and will be captured once visited.
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.		This broad category is covered by our vast library and 25+ categories. We review this area very frequently due to ever changing trends in dangerous practice, games and challenges. Gore and violence content is assigned the highest severity score within the library.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation. . Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010		Specific efforts are carried out to ensure the library best reflects concerns around discrimination and the vilification of groups through hate speech. This also includes deliberate misappropriation of groups and faith.

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses		A dedicated 'Hacking' category is built into the platform. Areas of monitoring include attempts to circumvent filtering and monitoring. We also include coverage for the installation or running of malicious programs, Proxies, unregulated sessions, registry editor.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions		Mis / Dis Information both deliberate and non-deliberate is something Securus caters for. This area is given especial attention as it constantly shifting and changing in line with world events.
Pornography	displays sexual acts or explicit images		One of the core categories, Securus monitors for many forms of pornography including most recently AI content.
Self Harm and eating disorders	encourages, promotes, or provides instructions for self harm or eating disorders		Securus monitors for eating, self-harm, image health, lookmaxxing, harmful beauty trends & eating disorders both clinical and non-clinical types.
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		VAWG and Misogyny form a dedicated area of concern for Securus. Forums, trends and spaces are subject to monitoring to identify instances of VAWG.

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

Securus software monitors for inappropriate content against a series of words and phrases divided into pre-defined categories in our library, including but not limited to the content categories listed above. The words and phrases are graded to reflect their potential level of severity. Our library is built in conjunction with national organisations such as the IWF and CTIRU, customer safeguarding staff feedback and recognised safeguarding experts and consultants and is reviewed regularly to ensure it is up to date. It is fully customisable, allowing schools to add words and phrases that may be specific to a region, address local concerns, or reflect local dialect or slang. The Securus solution can monitor ALL activity across a school's network, whether using the school owned devices (PC's Laptops & Tablet devices) and devices brought into the school and being used by pupils and staff under a BYOD policy.

The Securus solution takes a screen capture of every incident whether via an internet web page or an application, showing what was displayed at the time, highlighting the word(s) which triggered the capture, the pupil user ID, the device being used and the data and time the incident took place. This can be reviewed via the Securus Cloud Console by the appropriate members of staff who then decide on the most appropriate actions to take, being Cloud based this means that the Securus Cloud Console is accessible anytime/anywhere to increase the ability of staff to respond quickly and in the most appropriate manner. Options for safeguarding and senior staff include the ability to add comments and notes to capture incidents which may be useful when forwarding captures to colleagues, print or save captures and export captures directly into other safeguarding recording tools such as MyConcern and CPOMS. Alerts can be defined and managed by schools

DSLs themselves or via the Securus support team upon request, they are normally configured as part of the initial implementation and can then be updated or changed as required. Criterion for alerts, which are automated, is comprehensive and can be setup for many specific and non-specific scenarios such as those involving high severity incidents for a specific category or any incidents for high-risk individuals or groups. Alerts can be directed to any specific staff member or group of staff whose contact details are held, and they can be notified by email and also by telephone and even SMS for the highest severity alerts. In this way Securus not only helps schools to intervene in a timely and knowledgeable manner should the need arise but also helps to educate their pupils in the responsible use of technology. The solution will also enable the school to meet Government statutory safeguarding requirements and Ofsted or ISA inspection safeguarding criteria. Securus is designed to monitor online activity and behaviour rather than block access even though this capability can be configured if the school wishes. As described above, any inappropriate activity that registers against our proprietary library will be recorded via a screen "capture", the necessary staff can be alerted to review the capture and take the appropriate action. Securus does not over block, however, the system can be fine-tuned to reflect local requirements and needs, this includes "exclusion" functionality which can combine certain applications with specific criteria in order to determine whether or not to monitor, specific groups can be excluded, applications and websites can be whitelisted and the monitoring itself can be "dialled up or down" to adjust its sensitivity. Securus responds to the actual needs of the school whilst still ensuring the importance of identifying activity and using this information to educate the pupils about digital resilience and providing the school with the assurance they are protecting themselves in the future.

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. Further situations may warrant additional capability, for examples boarding schools or community based access		The Securus platform is highly configurable with custom user profiles and groups to reflect any age-appropriate structure such as year groups or other specific groups within a school such as High-Risk users or boarders. This flexibility extends to profiling of specific categories of monitoring against any of the age groups configured including alerts which can be set against these groups and are then routed to specific members of staff to follow up and action. This can all be controlled centrally which is particularly useful for multi academy trusts or schools' groups.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Alerts can be defined and managed by schools DSLs themselves or via the Securus support team upon request, they are normally configured as part of the

		initial implementation and can then be updated or changed as required. The criteria settings for alerts, which are automated, are comprehensive and can be setup for many specific and non-specific scenarios such as those involving high severity incidents for a specific category or any incidents for high-risk individuals or groups. Alerts can be directed to any specific staff member or group of staff whose contact details are held in the system, they can be notified by email and also by telephone and even SMS for the highest severity alerts.
• 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.		Activities for monitored users and supervisors, typically the designated safeguarding lead are logged within the software. Audit trails can be exported assuming sufficient permissions are in place.
• BYOD (Bring Your Own Device) – if adopted by the school and the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		Securus NET is our BYOD monitoring software solution which is installed at the network level to monitor ALL BYOD devices connected to the school Wi-Fi. BYOD devices are only monitored within the school location and hours. Information captured is sent from BYOD devices to our secure cloud server and can be reviewed within the Securus Cloud Console by the appropriate staff. Should monitoring beyond the school hours and away from the school location be required then we would recommend Securus XT for Windows, Securus XT for Chrome or Securus Browser for iOS, our device-based solutions.
• Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision		The capture data stored includes all the necessary information including the device, user ID, the words and phrases captured,

		severity grade and is date and time stamped. The Securus data is stored in a secure cloud UK datacentre which operates the highest levels of Information security and is ISO 27001 complaint. Our backup routine is constantly running with built in fail safes and data can also be exported out of Securus for saving elsewhere as part of existing school archives if required. We offer a standard data retention policy which can be adjusted to suit any individual school or MATs requirement.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		We offer native client applications for Windows and Chromebooks devices, an iOS browser for iPad devices. We also have a network-level solution to accommodate other devices & operating systems such as MacOS, Android and any other internet capable device and to provide coverage where software cannot be directly installed to the end device such as personal devices the school allows pupils to use as part of a BYOD policy. Thanks to our novel design, the network-level solution monitors any internet capable device and or its operating system. The solution can be customised to inspect and report on selected sites only and furthermore, and uniquely, produces a screen capture of inappropriate activity, the only design of its type that will provide true monitoring compliance and performance.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		It is a simple process for each school to add or amend keywords or phrases within its own custom library. The main Securus proprietary library, built in conjunction with national agencies such

		as IWF and CTIRU, is centrally controlled by Securus but the school can still edit some of the attributes of those words such as whether or not to monitor for their school.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		The Securus platform supports the central control and deployment of profiles and policies to multiple sites who can be represented within the Securus Cloud Console in a hierarchical organisation manner to reflect the group or muti-site structure in place. The level of oversight, system supervision and general access can be controlled and configured centrally and is configurable all the way down to an individual Securus user. The Dashboard offers a graphical representation of user activity by configurable date range. These graphs are generally used when reviewing the effectiveness of monitoring profiles. Every page element is interactive and the graphics themselves can be exported into a summary report. These graphs can be viewed at any level within the organisation structure such as overall MAT level, school groups, individual school or year group level.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).		Harmful images are discovered and monitored as part of our standard capture technology triggered by our library of keywords and phrases. Image only detection is outside of our current visible product roadmap.We are dedicated to unparalleled standards in typed and witnessed language content.
• Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the		We offer an application model for Chromebooks, Windows and iOS devices.

application of appropriate configurations for individual users.		Chromebook users are identified through workspace Gmail accounts or display names if preferred. Windows users are identified from their domain login details or local username. iOS users are identified from the schools MDM accounts or by way of QR code scanning. This solution allows schools to assign a unique QR code to each monitored person for easy sign on and subsequent user identification. Users on NET (BYOD Proxy) can be identified using a captive portal which will prompt the person mandatory login details when signing onto the monitored network. With users identified and segregated where appropriate, schools can introduced differing monitoring and library settings for individuals and groups.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		The Securus solution has an Acceptable Use Policy (AUP) that appears as soon as the user connects to the Wi-Fi or uses their device, and the user must accept the AUP to allow online access. The standard AUP supplied can be customised by each school to reflect their own wording and the school can have a different AUP for both online and offline access. We provide full guidance in the setup and deployment of the AUP to ensure all users are fully aware monitoring is in place.
• Mobile and app content – mobile and app content is often delivered in entirely different		We monitor iPads, Chromebooks and Windows

mechanisms from that delivered through a traditional web browser. To what extent does the monitoring system operate across mobile devices and app content. Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this.		devices with an application. Our BYOD solution for mobile and personal devices will monitor all browser activity but does not include apps that use proprietary certificates.
• Multiple language support – the ability for the system to manage relevant languages?		Whilst the default language is English, Securus can support and detect non-English words added to the library, and we can also implement full foreign language libraries if required.
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		Alerts can be defined and managed by schools DSLs themselves or via the Securus support team upon request, they are normally configured as part of the initial implementation and can then be updated or changed as required. The criteria settings for alerts, which are automated, is comprehensive and can be setup for many specific and non-specific scenarios such as those involving high severity incidents (level 5 being the most serious), for a specific category or any incidents for high-risk individuals or groups. Alerts can be automatically directed by email to any specific staff member or group of staff whose contact details are held in the system, they can also be notified by SMS for the highest severity alerts.
• Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users. Monitoring should focus on school-owned and managed devices. When shared devices are used, schools must ensure users log in individually. This allows monitoring systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.		Securus XT for Windows, Securus XT for Chrome and the Securus Browser for iOS will monitor school managed devices both in school and off site. Use of the school configured AUP will ensure the user is aware that they are being monitored even if off the school premises such as at home. Any captured activity will be sent

		immediately to the Securus Cloud Console for review. Being cloud deployed means that Safeguarding staff can access the Securus Cloud Console to review and manage captures generated anytime and from anywhere.
• Reporting – how alerts are recorded within the system?		Securus reporting is fully customisable and will allow designated users to set up scheduled email reports, based on differing criteria, on a daily/weekly/monthly basis. Alerts are also logged as an audit record.
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity		We offer full integrations with CPOMS and MyConcern allowing schools to export activity directly to their case management platform. It is also possible to export captures in a PDF style report for attaching to other case management platforms.

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Flexible, pro-active alerts can be defined against several criteria including specific users, capture source and the nature of activity detected. Alerts can be issued to individuals or groups of people within an organisation. As part of the full monitoring solution, email alerts are sent as soon as activities of concern are detected. The service team will also send an optional SMS message and will call immediately should the capture require attention with urgency. The Securus SLA details who are the primary and secondary contacts at the school and for what level of data and alerts they should be notified. Upon request, the service can support a degree of tailoring to allow schools to meet any specific safeguarding requirements.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

New engagement models and software modules are being released all the time to enhance our support to schools and DSLs in particular. Securus integrates with Microsoft AD for the automatic synchronisation of pupils (and staff) into their correct schools/year groups and dynamically updates the grouping even when pupils change AD groups mid-year. Securus also integrates directly with both MyConcern and CPOMS safeguarding recording solutions, totally in the control of the DSL this saves an enormous amount of time and duplication of data and information. Both our self-service and our fully managed solution are options available to our customers. All of the functionality described in this response is available whichever option the school chooses. The Securus Fully Managed Solution (FMS), however, combines the best of both worlds, our highly functional and comprehensive software capable of monitoring all devices alongside our human moderation service which helps to reduce the day to day workload for busy DSLs whilst alerting them to the captures of most concern and allowing them to fully engage with and support their safeguarding policy as laid out by their governing body and in compliance with their statutory

duties around Keeping Children Safe in Education. This collaborative approach between our human moderators and the local school staff and safeguarding team is increasingly popular with many of our customers, some examples of feedback include: “My feedback is simple –the service saves me potentially hours of additional work, is very cost effective, I am very happy with the service. In a nutshell – perfect” Headteacher - Community Primary School. “Securus Full Monitoring has without doubt made our job far easier than it was previously and more importantly has enabled us to identify more concerns than before. Having Securus in operation 24 hours a day every day gives peace of mind to the designated safeguarding team, which is particularly important at a time when we have loaned out over 300 laptops to students and another one hundred to staff during this second period of remote learning. I would recommend this service to any school without hesitation.” Director of Inclusion & DSL - Catholic Secondary School

How does your monitoring system identify and respond to activity involving Generative AI technologies (e.g. AI prompts, content creation, or platform use)?

In your response, please explain how your system captures or analyses user interactions with Generative AI tools; to what extent logs or alerts reflect potential safeguarding risks associated with AI-generated content (such as harmful prompts or inappropriate use of image and text generation); any known limitations—whether technical, privacy-related, or device-specific—that may affect your system’s ability to monitor such activity; and what guidance you provide to schools to support their understanding and management of Generative AI-related risks.

The software inspects both the screen and keyboard buffer to detect attempts to search and use AI GEN platforms. This is achieved in part by the software’s design and the contents of the global library. Recent updates to the global library include the addition of specific AI platform names such as Chatgpt, Gemini and co-pilot. We always ensure compliance with recent KCSIE guidance with respect to safeguarding, but we also alert to AI / academic misconduct. Attempts to ‘cheat’ with and ‘copy’ from AI generative text is also an area we aim to detect. AI is also used to reduce false positives and better identify potentially harmful activities. Our team of moderators use AI modules to better train the system to identify genuine developing concerns. Additionally, whilst we don’t inhibit access to websites, as part of the full monitoring service we will also notify the Network Manager to websites that we believe should be marked for blocking. We host frequent meetings on safeguarding subjects including the misuse and dangers of AI.

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	Bernard Snowe

Position	CEO
Date	8 June 2026
Signature