Appropriate Monitoring for Schools

May 2023

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	LAN2LAN House, Brook Way, Leatherhead, Surrey, KT22 7NA
Contact details	Bernard Snowe Bernard.snowe@securus-software.com Tel: 0330 124 1750
Monitoring System	Securus XT for Windows, Securus XT for Chrome, Securus NET, Securus FMS Full Monitoring Service
Date of assessment	03/07/2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	

Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

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.
• 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.
• Confirm that monitoring for illegal content cannot be disabled by the school		Multiple preventative designs to ensure that the monitoring of illegal content is maintained. This includes tamper proofing and hidden library elements.

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
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		The Securus software monitors for inappropriate online content against a series of words and phrases divided into pre-defined (and custom) categories in our library. The words and phrases are graded to reflect their potential level of severity. Alerts can be configured to notify staff of any incidents that require intervention and action. Grooming (which also covers child abuse) and Radicalisation / Terrorism categories which are standard would certainly be

			considered content which is Illegal.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		As above – Bullying is a standard category
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		As above – Grooming is a standard category and would cover content that includes Child Sexual Exploitation.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		As above – Discrimination is a standard category
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		As above – Drugs, which includes Substance Abuse, is a standard category
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		As above – Radicalisation, which includes content classed as Extremism in nature, is a standard category
Gambling	Enables gambling		This is a standard category in Securus
Pornography	displays sexual acts or explicit images		As above – Pornography is a standard category
Self Harm	promotes or displays deliberate self harm		As above – Self Harm is a standard category
Suicide	Suggest the user is considering suicide		As above – Suicide is a standard category
Violence	Displays or promotes the use of physical force intended to hurt or kill		As above – Violence is a standard category

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 also 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 and integrates with teamSOS for additional alerting capability.

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 white listed and the monitoring itself can be “dialled up or down” to adjust its sensitivity.

In this way the system 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		The Securus platform is highly configurable with custom user profiles and groups to reflect any age appropriate structure such

capability, for examples boarding schools or community based access		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		Activities for monitored users and supervisors, typically the designated

transparency and that individuals are not able to make unilateral changes.		safeguarding lead are logged within the software. Audit trails can be exported assuming sufficient permissions are in place.
• BYOD (Bring Your Own Device) – if 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 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, our client-based solution.
• 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

		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 and we also have a network-level solution to accommodate iOS, MacOS 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 is able to monitor any internet capable device and or its operating system including iOS, MacOS, Android & Linux. 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.
• 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.
• 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.		Securus XT will monitor school managed devices both in school and also off site / any location that the school owned device has been used. 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. Being cloud deployed means that Safeguarding staff can access the Securus Cloud Console to review and manage captures generated anytime and from anywhere. This has been seen to be particularly useful over the past two years during the Covid pandemic when pupils have continued to study from home and the school is therefore able to continue to monitor and safeguard them.
• 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.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		All captures generated include a full screenshot of the visual content which highlights the key word which triggered the capture and also up to 10 other associated words if any exist in the screenshot. OCR (screen scanning) is used to capture and analyse screenshots and provide context to safeguarding staff. The software also includes an image analysis design providing richer meta / contextual information.

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 service, 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 service 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 Service (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

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 Snow
Position	CEO
Date	3th July 2023
Signature