Appropriate Monitoring for Schools

June 2021

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 they "should be doing all that they reasonably can to limit children's exposure to the above 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	Exa Networks
Address	100 Bolton Road, Bradford, BD1 4DE
Contact details	mark.cowgill@exa.net.uk & 0345 1451234
Monitoring System	SurfProtect Quantum & Securus
Date of assessment	6th October 2021

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	🟩	Exa have been full members of the IWF for over fifteen year
● Utilisation of IWF URL list for the attempted access of known child abuse images	🟩	And the CAIC URL List is included as standard on SurfProtect Quantum and cannot be deactivated
● Work with CTIRU ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’	🟩	Yes, the CTIRU assessed list is included with SurfProtect Quantum and cannot be deactivated

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 the 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. Illegal is a standard category.
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 - Child Sexual Exploitation is a standard category.
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 / Substance Abuse is a standard category
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	As above – Extremism is a standard category
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

Full details on the SurfProtect, filtering side, of monitoring, can be found on our Filtering submission.

Securus software monitors for inappropriate online content against a series of words and phrases divided into pre-defined categories in our library. The words and phrases are graded to reflect their potential level of severity. The library is built in conjunction with national agencies such as IWF & CTIRU 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. The Securus software solution can monitor ALL activity across a school's network, whether using the school devices (PC's Laptops & Tablet devices) and/or any devices, such as Tablet PC's and Smartphones, 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, showing what was displayed at the time, who was involved, the device being used and when the incident took place. This can be reviewed in the Securus Portal by the appropriate members of staff who then decide on the most appropriate actions to take. In this way they help the child and help the school to meet Ofsted's safeguarding criteria. Alerts can be configured to notify staff of any incidents that require intervention and action.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Full details on the SurfProtect, filtering side, of monitoring, and how we do not over block access can be found on our Filtering submission.

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 then they can take the appropriate action. Securus does not over block since pupils may try and circumvent the blocking rules It is more important to identify the activity and use the information to educate the pupils about digital resilience and provide them with the opportunities to protect themselves in 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	🟩	The system is very flexible, custom groups

age. 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	🟩	can be set up to reflect any structure such as year group or age or other specific groups within a school such as High Risk users. The alerts can be set against these groups and can also be routed to specific members of staff to follow up and action.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	Alerts can be defined and managed by schools themselves or via the Securus support team using a change request. Criterion for alerts is comprehensive and can be setup for many specific and non-specific scenarios.
• 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 the 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 school. Information captured is sent from BYOD devices to our secure cloud server and can be reviewed within the Securus 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 includes all the necessary information including the device, user, the words and phrases captured, severity grade and is

	🟩	date and time stamped. Data is stored in our secure Cloud UK datacentre or can be implemented locally on the school server. Data can be stored on the server for as long as required and this can be configured on a per school basis.
• 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 provide both a client device version, Securus XT, which is installed on Windows and Chromebook devices and a network version, Securus NET, which can monitor ANY device connected to the establishment Wi-Fi
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	It is a simple process for each school to add or amend keywords or phrases within its own custom library. The Securus proprietary library built in conjunction with national agencies such as IWF and CTIRU, is controlled by Securus.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	The Securus platform supports the central deployment of profile and policies to multiple sites. Level of oversight and access is configurable per Securus user
• 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, this can be customised by each school to reflect their own wording. We advise all schools to ensure all users are fully

	🟩	aware that they must accept the AUP to allow online access.
• 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 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 generated once any capture has been made, dependent on what criteria has been set. This is based on the severity score attached to each word and phrase. The alerts can be set using our 'Alert trigger' feature. Once a set of criteria has been met, an alert will be sent to the designated recipient/recipients alerting them accordingly. The alert criteria are set by the school after training and consultation. This is vital in certain situations to protect an individual pupil.
• 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.	🟩	We provide both a client device version, Securus XT, which is installed on Windows and Chromebook devices and provides the remote monitoring regardless of location, and a network version, Securus NET, which can monitor ANY device connected to the establishment Wi-Fi
• 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)	🟩	

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

Securus is an online safeguarding solution that monitors all activity at places of learning, ensuring that young people, especially those identified as vulnerable or at risk, are safeguarded against the wide range of threats they face whilst online.

- Securus provides a solution for all education establishments, regardless of number of pupils, type of school/establishment or devices on the network including support for BYOD.
- Securus highlights a wide range of online behaviour including severity levels, types of incidents, top users, top phrases, high risk users and other specific capture reports and trends.
- Securus alerts school authorities to anything that suggests a child may be at risk or is breaching acceptable use policies.
- Securus keeps pupils' safe by alerting staff to any areas of concern and provides the evidential information for the school to fulfil their obligations as outlined by the regulatory authorities.
- Securus helps provide the means to educate young people about the importance of online safety, thereby contributing to their digital resilience.
- Securus helps define boundaries so that students understand what is expected of them in line with the acceptable use policy and enables staff to act on any infringements.
- Securus helps pupils feel safe because they know that staff will be made aware of any threatening behaviour.
- Securus gives teachers the information to educate their students on the difference between acceptable and unacceptable behaviour.
- At the heart of Securus is a proprietary library divided into various categories, containing all our key words and phrases. The library is reviewed and updated in conjunction with safeguarding and other law enforcement agencies

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	Mark Cowgill
Position	Co-Founder & Director
Date	7th October 2021
Signature	M Cowgill