Appropriate Monitoring for Schools

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet IWF

April 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 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	Renato Software Ltd.
Address	Sterling House, Wheatcroft Business Park, Edwalton, Nottingham, NG12 4DG
Contact details	0115 857 3776 m.payne@renatosoftware.com
Monitoring System	Senso Safeguard Cloud
Date of assessment	28/04/2023

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	🟩	Senso is a member of the IWF and actively communicates with them.
● Utilisation of IWF URL list for the attempted access of known child abuse images	🟩	Senso blocks IWF URLs and logs attempted access, without sharing the URL details or taking screenshots.
● Work with CTIRU ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’	🟩	Senso blocks access to CTIRU unlawful terrorist content.

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	🟩	Senso helps protect students by providing real-time analysis of text and keystrokes, with an additional Artificial Intelligence (AI) to analyse screenshots for visual threats. Our libraries are graded into five different levels of severity, and match conditions allow us to specify whether terms are considered violations alone or in the presence of other terms. Alerts can be configured to notify appointed staff members of any severe or critical violation that may require immediate intervention. This category meets the requirement for blocking “illegal” content.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	As above; the Senso system has dedicated resources for monitoring and managing “bullying” content.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet	🟩	As above; the Senso system has dedicated resources for monitoring and managing “child sexual exploitation” content.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	As above; the Senso system has dedicated resources for monitoring and managing “discrimination” content.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	As above; the Senso system has dedicated resources for monitoring and managing “drugs / substance abuse” content.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	As above; the Senso system has dedicated resources for monitoring and managing “extremism” content.
Pornography	displays sexual acts or explicit images	🟩	As above; the Senso system has dedicated resources for monitoring and managing “pornography” content.
Self Harm	promotes or displays deliberate self harm	🟩	As above; the Senso system has dedicated resources for monitoring and managing “self-harm” content.
Suicide	Suggest the user is considering suicide	🟩	As above; the Senso system has dedicated resources for monitoring and managing “suicide” content.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	As above; the Senso system has dedicated resources for monitoring and managing “violence” content.

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

Senso helps schools meet safeguarding requirements and protect at-risk students by providing real-time analysis of text and keystrokes, as well as implementing an Artificial Intelligence (AI) image scanner to analyse screenshots for visual threats and harmful imagery. In addition to monitoring across a host of applications and operating systems as standard, Senso also has the capability to monitor Microsoft Teams chat in real time, allowing teachers and Designated Safeguarding Leads (DSLs) to react quickly to harmful or high-risk interactions. Senso’s logging and reporting functionalities are focused on student and user safety, creating a safe and user-friendly environment with pro-active characteristics to help inform and alert the appropriate parties, typically the DSLs, when issues occur. Senso is entirely cloud-based which brings greater agility to meet rising demands for new technology while driving new innovations to make distance learning safer and more resilient for the future.

Senso works with the Internet Watch Foundation (IWF), The Counter Terrorism Internet Referral Unit (CTIRU), Samaritans, Tech Against Terrorism, and the UK Safer Internet Centre (UKSIC), along with leading multi-academy trusts, local authorities, independent e-safety experts and our community of Senso schools to be able to continuously update our keyword libraries and respond to current events and emerging trends. Senso benefits from an in-house linguist with specific safeguarding expertise, we are now officially partnered with Birmingham City University as part of a UK Research and Innovation ‘Knowledge Transfer Partnership’ to help make our safeguarding offering as effective and cutting-edge as possible. Our keyword libraries are regularly updated and are informed by the UK Department for Education’s statutory guidance ‘Keeping Children Safe in Education’. Finally, we are proud to be partnered with the nationally-leading South-West Grid for

Learning (SWGfL) who work with Senso to provide an outstanding assisted monitoring service to schools and trusts in the UK.

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

Senso's monitoring software is designed to work alongside an internet filter and give schools the peace of mind that educational content can be provided without compromising on immediate alerting for potentially harmful or high-risk terms. Senso offers a flexible and customisable approach, allowing for age-/time-/user-appropriate monitoring. Schools can create custom keyword libraries for their own specific purposes, can whitelist terms where needed, and can add customised blocks on either a permanent or an ad hoc basis to an individual, group, or the entire school if they choose. Raising awareness as opposed to over-blocking allows the school to have frank and open discussion with at-risk individuals.

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. 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	🟩	Senso.cloud is a highly configurable monitoring solution that can apply different sets of safeguarding policies to different sites according to e.g. school/site, year, user group, student, device, or directory information.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	DSLs at Senso schools manage the system alerts and execute any required actions. Senso Safeguard Assisted Monitoring, in partnership with SWGfL, is also available to provide direct support as required. The system can be configured to delegate access to any member of staff, internal or external to the school, or trusted third-party companies if so desired. Senso manages the physical storage, integrity, disaster recovery and security of the system alerts. In the case of 'critical' or 'urgent' severity-level violations, secure email alerts are sent directly to

	🟩	DSLs' inboxes at the time of occurrence.
• 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	🟩	Senso can be installed on BYOD machines that are running Microsoft Windows 10, Chromebooks, iOS and MAC. The Senso client MSI may be installed manually or pushed out through a school's compliance gateway. The school is the main contact for supporting BYOD devices. The school may raise support queries for the BYOD device in question but must remain as intermediator. Since Senso is a truly cloud-based solution, monitoring and logging will continue to work even away from the school. As the device is owned by the student they may stop the Senso service at any time which will disable all Senso monitoring activities as is the case with any software.
● 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	🟩	Senso uses Microsoft Azure to provide its cloud technology. Data is stored in Data Centres in the EU. The retention period is determined by the customer, length of subscription, or in the case of a legal investigation, the Police or courts.
• 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 following Operating Systems are fully supported: - Windows 10, 64 Bit - Chromebook - iOS - MacOSX
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	Schools can add their own keyword libraries or whitelist over existing Senso terms if required, except in the case of illegal content identified by the IWF or CTIRU. Senso is a cloud-based solution, meaning that it can be

	🟩	deployed flexibly and without the need for on-site servers. It also means that multi-academy trusts, for example, can remotely manage all schools from one overarching account or may delegate rights to individual schools to manage their own students and staff. Being cloud-based means that these changes can be implemented quickly and easily.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Senso offers a flexible, hierarchical approach for managing sites from one easy-to-use web portal, whether this is multiple sites at once or an individual school. A central policy can be deployed at the top level (i.e. Trust/MAT level) that will then be delivered to all schools. This policy can either be made mandatory across the trust or can be overridden at an individual school. This allows for a single update to be rolled out for all schools. Each school may have additional policies if they require. The Senso dashboard provides a top-level (Trust/MAT) overview of all violations across a single or multiple site setup, meaning that Senso can deliver unparalleled insights into users' actions and behaviour. One-click drilldown improves speed and effectiveness to get to the core of the problem as quickly as possible.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	Senso can display multiple AUPs (Acceptable User Policies) dependent on group membership when the

	🟩	device is logged in to. The user must read and accept the terms of the AUP before they can proceed with their session. If they do not accept the terms they will automatically be logged out of the operating system.
- Multiple language support – the ability for the system to manage relevant languages?	🟩	Senso is based on Unicode characters which allows us to support any language including those with non-Latin alphabets.
- 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 are triggered by keyword terms and their detection settings. All violation captures within the system are assigned a severity rating range from 1-5, enabling schools to prioritise the system output easily. In addition, violations can be filtered according to a range of priorities, including specific user groups, the device name, username, word or phrase mention, severity level, application, and time frame. For instance, a Designated Safeguarding Lead may choose to see all alerts with severity classification of 'urgent' or 'critical' (with immediate action required) for all schools in a trust, while a teacher in a single school may only choose to see alerts for a smaller subset of students.
- 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.	🟩	Thanks to Senso's cloud-based design, students are able to be monitored regardless of their location as long as they have an internet connection. Relevant school staff are also able to access this system from any device with an internet connection and internet browser.

• Reporting – how alerts are recorded within the system?	🟩	Not only are Senso's safeguarding alerts ultra-secure, in that they are available only to those with the required access privileges, but they are also read-only which means they cannot be tampered with. Senso requires three signatures from a school's senior management team or a court order before it will action a request to remove certain violations from its database. Senso takes security very seriously and uses industry-standard protocols to encrypt data in transit as it travels between devices and Microsoft datacentres, which are used to host the Senso servers. Once an alert has been triggered, the data about the alert is encrypted and securely transferred to the Senso cloud servers for storage, whilst recording various information about the alert including IP Address, Device Name, Username, Phrase, Actions, Date, Time, Screenshot, Category, Severity Level, Application used, etc. If the device is not connected to the internet and a violation is triggered the violation is stored locally within an encrypted database. Once the device regains internet access it performs a smart transfer of the violations to the Senso cloud servers.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)	🟩	Upon a keyword violation capture and screenshot, Senso Safeguard Cloud will analyse the screenshot using AI-driven threat detection. The AI system is trained to determine whether the

	🟩	screenshot contains images that match the following categories: - Alcohol - Drugs - Extremism - Gore - Porn - Swim/Underwear - Weapons Any images detected as potentially harmful or inappropriate will be marked as a visual threat and highlighted at the top of the violation dashboard.

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

The Senso platform integrates with the following:

- Clever
- CPOMS
- Google Classroom
- Microsoft Azure AD Groups
- Microsoft Teams Chat (Monitoring)
- Microsoft Teams (Sync)
- MyConcern

In response to user requests, we are also currently developing an API for direct integration with Microsoft Power BI.

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	Michael Payne
Position	Director of Operations
Date	28-Apr-2023
Signature	