Appropriate Monitoring for Schools

August 2020

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. Children should not be able to access harmful or inappropriate material from the school or colleges 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	Talk Straight Ltd / Schools Broadband
Address	2-4 Dansk Way, Ilkley LS29 8JZ
Contact details	01133 222 333, info@schoolsbroadband.co.uk
Monitoring System	Senso.Cloud
Date of assessment	28/08/2020

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 is in active communication with them.
• Utilisation of IWF Hash list to identify the storage or transmission of known child abuse images		Yes
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes

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		Talk Straight Senso.Cloud services helps protect at-risk students by providing in realtime text analysis, keystrokes, and Artificial Intelligence (AI) to analyse screenshots for visual threats. Our libraries are graded into five different levels of severity. 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".
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		As in the explanation above, the category requirements for 'Bullying' are met in Senso.Cloud.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		As in the explanation above, the category requirements for 'Child Sexual Exploitation' are met in Senso.Cloud.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		As in the explanation above, the category requirements for 'Discrimination' are met in Senso.Cloud.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		As in the explanation above, the category requirements for 'Drugs/Substance abuse' are met in Senso.Cloud.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		As in the explanation above, the category requirements for 'Extremism' are met in Senso.Cloud.
Pornography	displays sexual acts or explicit images		As in the explanation above, the category requirements for 'Pornography' are met in Senso.Cloud.
Self Harm	promotes or displays deliberate self harm		As in the explanation above, the category requirements for 'Self-Harm' are met in Senso.Cloud.
Suicide	Suggest the user is considering suicide		As in the explanation above, the category requirements for 'Suicide' are met in Senso.Cloud.
Violence	Displays or promotes the use of physical force intended to hurt or kill		As in the explanation above, the category requirements for 'Violence' are met in Senso.Cloud.

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

Talk Straight provide Senso.Cloud which helps schools meet safeguarding initiatives and protect at-risk students by providing in real-time text analysis, keystrokes, and Artificial Intelligence (AI) to analyse screenshots for visual threats. Being focused on student and user safety; creating a safe environment with pro-active and/or reactive characteristics to help encourage inclusivity and alert appropriate parties, such as teachers, when issues occur.

Senso was forged from the cloud 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), Tech Against Terrorism, UK Safer Internet Centre (UKSIC) along with leading multi-academy trusts, local authorities, independent e-safety experts and our community of Senso schools to continuously update our keyword and AI libraries which are based on The UK Department for Education's statutory guidance 'Keeping Children Safe in Education'.

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

Senso is constantly moving forward with new technologies and does not block any website out of the box unless it is illegal. Schools can add custom blocks on a persistent or an ad hoc basis to an individual, group or the entire school if they choose. Raising awareness versus over blocking gives the school the opportunity 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 policies to different sites either based on school, year, group, student, device, or Directory info.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		School DSL's manage the system alerts and any required action that needs to be taken. The system can be configured to delegate access to any member of staff, internal or external to the school, or 3rd party companies if so desired. Senso manages the physical storage, integrity, disaster recovery and security of the system alerts.
• 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.Cloud can be installed on BYOD devices that are running Microsoft Windows Operating Systems 8.1 or 10 and Chromebooks. 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. Since 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) stored and for how long		Senso.Cloud 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.
• 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 8.1, 32/64Bit Windows 10, 32/64Bit Chromebook with more in due course.
• 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 for illegal content identified by the IWF or CTIRU. Senso is a cloud based solution, the flexibility to manage keywords for other schools under the same umbrella is possible, with the added ability to have an overarching safeguarding offer manage all schools but give rights to individual schools to manage their own school.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Senso has been designed for with multi-site in mind from the start but works equally as well within a single school. With Senso you can uniquely use a top-down approach to manage all your schools from one easy to use web portal or allow each school to manage their own. The choice is up to you. Deployment of a Central Policy: Setup one policy at the top level (Trust/MAT) that will then be delivered to all your schools. You can then decide if this policy is mandatory or can be overridden at an individual school. This allows you to make a single update for all

		schools. Each school can have additional policies if they require. Dashboard: With a top-level (Trust/MAT) overview of all violations across a single or multiple site setup, Senso can deliver unparalleled insight 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 AUP's (Acceptable User Policies) dependant on group membership when the device is logged into. 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 log 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 Non-Latin languages.
• 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 captures within the system are assigned a severity rating range from 1-5, enabling schools to prioritise these easily. In addition, schools or Multi-Academy Trusts may give access to only see certain school or groups within that school. For instance, the Lead Safeguarding Officer may want to see all alerts with Severe classification (immediate action required) for every school in the Trust. While a teacher in a single school only needs to see

		alerts for a smaller subset of student.
• Reporting – how alerts are recorded within the system?		Senso raises the standard of handling safeguarding alerts. Not only are our safeguarding alerts ultra-secure they are also read only which means they cannot be tampered with. Senso requires three signatures from the school's senior management team or a court order before it will action a request to remove certain violations. 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…. For any reason 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.

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

Senso Platform integrates with the following. • Clever

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

Senso Concern Toolbar allows users to report a concern directly from their desktop as known user or anonymously with customised message and screenshot. Senso® Assisted Monitoring service applies the capability of award-winning online safety specialists to assist schools in managing their Senso safeguarding technology. Assistance is an important and powerful descriptor as the service works in collaboration with each school rather than seizing responsibility; partnering the capability and capacity of online safety specialists with local school child safeguarding people and processes. Specifically, the service has specialists continually review the Senso alerts to identify harmful incidents that warrant immediate intervention (where harm is apparent), then actively engage nominated staff at the school, both of the incident together with a suggested intervention.

The case managers, supported by child protection specialists, are skilled in assessing the alerts, assimilate the risk and harm, and identify a response or escalation. This analysis of each alert is focused on the context of the Violation, the usage patterns of the specific user, and any other relevant factors and supporting information.

The union of this service with local school child safeguarding, recognises that school staff may have a range of distractions that prevent them from applying the sole attention to the management of their monitoring system. In addition, when incidents occur, school staff are likely to appreciate the suggestions about managing the incidence in context of their own child safeguarding policies and procedures. It also allows schools to manage other incidents that don't warrant the immediacy of intervention at their own discretion. Examples clearly demonstrate that children benefit from this 'assistance'.

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	David Tindall
Position	Chief Executive Officer
Date	28/08/2020
Signature