Appropriate Monitoring for Schools

May 2023

Monitoring Provider Checklist Responses

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	Smoothwall (part of Qoria)
Address	Second Floor, 2 Whitehall Quay, Leeds, LS1 4HR
Contact details	https://www.smoothwall.com/education/contact-us/
Monitoring System	Smoothwall Monitor
Date of assessment	30/08/2023

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, Smoothwall is a member of the Internet Watch Foundation and implement the IWF CAIC list.
• Utilisation of IWF URL list for the attempted access of known child abuse images		The images we see are generally screenshots, and as such aren't suitable for hashing. Hashing is able only to match images with minor changes, and as such cannot hope to match (eg.) an image and that image screenshot in a user's browser.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall has worked with CITRU for many years across both filtering and monitoring
• Confirm that monitoring for illegal content cannot be disabled by the school		It is not possible to fully disable monitoring without uninstalling the system

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		There are 3 themes that cover this requirement - a specific theme on Terrorism, a specific theme on CAI and an additional theme on Grooming. Monitor uses a detailed process to ensure that we alert Users to activity within these themes, without propagating any images that may have been shared.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		The "Bullying" theme includes both entirely online bullying, and references to physical world counterparts.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Smoothwall Monitor includes the detection of contact with monitored users for sexual purposes. Monitoring looks for signs of grooming and requests for sexual information or images. The "Oversharer" theme alerts in

			instances where a monitored user might be providing personal information online – their address, full name or phone number for example.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Bullying detection also includes monitoring of bigotry, hatred and discrimination.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Drug and substance abuse would be classified as “General Risk”, or in some cases “Vulnerable User” where the individual is at risk of exposure or has been exposed to drugs
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The “Terrorism/Extremism” theme is designed entirely for detection of terror and extremism content
Gambling	Enables gambling		Gambling would be classified as “General Risk”, or in some cases “Vulnerable User”
Pornography	displays sexual acts or explicit images		“Sexual Content” alerts will provide alerts when monitored users attempt to access or discuss pornography. Smoothwall recommends this is used in conjunction with a good quality web filter
Self Harm	promotes or displays deliberate self harm		The “Vulnerable user” theme includes detection of various activities related to self harm.
Suicide	Suggest the user is considering suicide		As with Self Harm, suicidal ideation ad discussion of or researching suicide related material is covered by the “Vulnerable User” theme. If a risk to life is suspected, the DSL will receive a phone call straight away – 24/7/365.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Violent material is covered by the Violence theme

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

Smoothwall Monitor is powered by a combination of AI and human moderation. The moderation team sees data from many sources, so new trends are picked up rapidly. AI is excellent at spotting unusual trends, and outlier data, providing comprehensive coverage. With human feedback into the AI, the system is constantly learning and improving

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		Monitor has several age group settings which are applied during onboarding. This alters alert thresholds and settings relevant to the age group chosen. Age group settings can be applied to specific Groups of users, allowing for granular control of Monitoring sensitivity.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Monitor allows fully customisable alert settings for the site or groups within the site. Alerts can be tailored for each Safeguarding user of the system, allowing them to chose the Groups they receive alerts for, and the severity at which they will be notified.
• 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.		Users are not able to perform any actions in the UI that would cause concern. For example they are not able to delete alerts from the database.
• 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		Monitor does not currently fully cater for BYOD. However if a student logs into their school Chrome account on a BYOD that activity would be Monitored.
• 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		Data is stored on our secure servers for a period of 15 months and then permanently deleted. Monitor's integration with all widely-used

		safeguarding record keeping systems allows Safeguarding users to automatically copy data across, providing longer term storage
● Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Monitor supports Windows, MacOS, iOS and ChromeOS. Customers are informed of this during the sales and onboarding process.
● Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		Schools have the option to feed back into the moderation system, however we do not permit individual words to generate an alert – this would usually result in many more alerts. The AI and human moderation components are part of a carefully calibrated system where new sources of alerts are added by our professional analysts.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Requirements for monitoring across all sites within a group of schools will be discussed during a customer's onboarding. Where centrally-managed policies are required they can be easily mirrored across sites, and central users can be given a variety of levels of visibility over their sites. Monitor's reporting tools are suitable for single sites and large groups of schools, and automatically display information on all sites the user has access to.
● Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Smoothwall provides assistance to customers in informing their users about monitoring with Smoothwall Monitor

● Multiple language support – the ability for the system to manage relevant languages?		Smoothwall Monitor is used across the UK, US and Australia. Monitor fully supports English and Spanish, and contains a number of keywords from many commonly-used 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 categorised on a scale of 1 to 5, initially by AI, then a human reviewer. Alerts are then sent according to theme and severity. Almost all events will trigger an email, some higher level events will trigger a phone call to the Safeguarding Team
● 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.		Monitored devices are actively monitored 24/7/365, whether the device is in-school or elsewhere. All activity on a monitored device will be analysed. Only school-issued devices and accounts are supported by Monitor. Smoothwall provides assistance to schools in making users and parents aware of monitoring.
● Reporting – how alerts are recorded within the system?		Alerts are recorded separately to capture information. All alerts are available in the portal and can be searched, linked through to associated screen captures. Permanent storage should be in the school's record management system. A full set of reports over time showing alert types and levels is available within the Monitor dashboard.

● Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		Images which accompany captures are reviewed by the moderation team.

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.

Smoothwall monitor only supports pro-active monitoring. Smoothwall believes this is the only way monitoring implementations can be successful. Automation is used to support the monitoring team in weeding out captures which are not harmful, and presenting the moderation team with the data in the most efficient way. The moderation team are all Smoothwall employees, fully DBS checked, and have the support of counsellors and the HR team. None are on a zero hours contract. The moderation team do not make decisions on the outcome, they are there to make sure you don't see false positives. As such, they are not trained safeguarders per se, rather operatives trained in understanding what they are seeing and wether a DSL or other safeguarder would need to be alerted.

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

As part of the wider Qoria group, Smoothwall offers a huge range of products and support for schools, including best in class Monitoring, Record Management, Classroom Management and Student Wellbeing tools. Additionally Smoothwall offers training and resources to promote safety in UK schools, including a school branded "hub" for parents and students.

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	Tracy Harper
Position	Product Director - Early Detection and Intervention
Date	31/08/23
Signature