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	**Censornet Ltd**
Address	**Matrix House, Basing View, Basingstoke, RG21 4FF**
Contact details	**Gareth Lockwood, VP Product, gareth.lockwood@censornet.com**
Monitoring System	**Censornet USS – Web Security Advanced**
Date of assessment	**24/10/2023**

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		Indirect member: zVelo Inc who provide our Web URL classification and analysis analysis have been a member since 2011.
• Utilisation of IWF URL list for the attempted access of known child abuse images		Our OEM partner zVelo implement the URL list and integrate into our Web Security module.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU option is enabled for education and public sector clients.
• Confirm that monitoring for illegal content cannot be disabled by the school		Default System Rules cannot be deleted. RBAC facilitates read-only access to Filter Rules.

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		Multiple sub-categories under Criminal Activities including Child Abuse Images, Hate Speech, Terrorism
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Numerous System Default Keyword lists maintained including Abuse, Discrimination, Profanities, Bullying, Radicalisation etc.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Numerous System Default Keyword lists maintained including sexual terms, mental health, abuse, anxiety etc. Custom keywords and profiles can be created to enhance this list.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Defined as extreme right and/or left wing groups, sexist remarks, racist remarks or racial slurs, religious hate, or the promotion of oppression of certain groups or individuals based on race, religion, nationality, political affiliation, gender, age, disability, or sexual orientation.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Pages that in any way endorse or glorify commonly illegal drugs, the misuse of prescription drugs, the misuse of inhalents, or any positive references to the culture of drug use whether specific drugs are mentioned or not. Includes sites giving non-clinical descriptions or stories about being high as well as blogs and other posts about getting high. crack, heroine, morphine etc.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Deep inspection of Social Media apps like Facebook, Twitter including keyword reporting; Web categories Hate Speech and Violence (described as Web pages that promote questionable activities such as violence and militancy)
Gambling	Enables gambling		Category includes Games that involve the winning or losing of money based on strategy and chance. Includes information, tips, strategies, and rules for gambling games.
Pornography	displays sexual acts or explicit images		Safe Search enforcement and Web Categories: Pornography, Sex & Erotic, R-Rated. Optional Image Filter module provides real time image scanning for pornographic content
Self Harm	promotes or displays deliberate self harm		Web Category Self Help & Addition, described as Web pages which include sites with information and help on gambling, drug, and alcohol addiction as well as sites helping with eating disorders such as anorexia, bulimia, and overeating
Suicide	Suggest the user is considering suicide		Multiple categories and keyword lists monitored including bullying, mental health, suicide, violence etc.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Web Category Violence described as Web pages that promote questionable activities such as violence and militancy

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

- Full visibility of Cloud Application usage and Social Media sites including capturing actions such as posting to social network sites and search engine terms
- Scans all accessed URLs for reputation based on Web Category
- On-demand lookup for unknown URLs / zero-day
- Integrated Anti-malware scanning
- MIME Type Scanning
- Counter Terrorism list enforcement
- Safe search enforcement – Google Safe Search, Google App Domain, Bing, Yahoo!, YouTube, YouTube for Schools
- Policy based control of Web categories and Safe Search
- Keyword lists to trigger policies, i.e. profanities, radicalisation, bullying. DLP module to filter based on file contents.

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		The platform supports several deployment methods and profile configurations. User/device profiles can be synced with Active Directory and segmented by group, or custom profiles can be deployed by segment.
Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Realtime Log Streaming supported in order to deliver events to 3rd party SIEM system. Actions/categories/events and rule violations can be categoried into different log priorities.
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.		All administrator actions and changes are logged for audit compliance. Administrators can also be segmented into roles limiting platform access and control.
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		This is achievable via a Captive Portal mechanism when the device is on the local network, or via VPN to the gateway for roaming users (requires MDM solution). In addition, we offer a Cloud Application

		Security module which has an App Catalog of hundreds of mobile and desktop apps that can be used to identify apps in use and control access to them.
● 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		Default is 90 days with auto-archive to CSV which is available for a further 12 months free of charge. The 90 day retention period can be extended for an extra free. Data is stored on highly available, high performance and globally distributed AWS infrastructure.
Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Device agents for Windows/Mac/Chromebook. Linux-based gateway for agentless connection. Logged activity includes device information, user, IP etc.
Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		Maintained keyword list accessible from platform settings. Non-system rules can be added/changed/deleted with appropriate permissions.
Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		AD integration enables sync with org structure and detailed granular reporting. Platform uses a multi-tenant and parent/child schema for centralised management.
Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Custom warning pages and templates can be created to inform and educate users when accessing web pages and content (and activity logged, or action triggered). A Best Practice guide is provided to institutions to further fine-tune the policies and configuration from the default. Users can be made aware of monitoring by creating a custom template for a pre-defined page (i.e. home page

		or intranet site) and setting the rule to allow access such that it is presented then passed.
Multiple language support – the ability for the system to manage relevant languages?		Over 100 languages are supported in the Web Security database
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?		Log Streaming functionality enables real-time alerting via a 3rd party SIEM system. Events can be logged natively using a priority tag. Scheduled reports can be customised and delivered via PDF to an email list on a regular cadence, e.g. hourly notification of high-risk activity or logs.
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.		This is achievable via a Captive Portal mechanism when the device is on the local network, or via VPN to the gateway for roaming users (requires MDM solution). Hours of operation can be configured in the policy engine. In addition, we offer a Cloud Application Security module which has an App Catalog of hundreds of mobile and desktop apps that can be used to identify apps in use and control access to them.
Reporting – how alerts are recorded within the system?		Extensive Web Activity audit reports and pre-defined charts. Scheduled reports can be created, customised and delivered to email lists on a regular cadence.
Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		

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.

Real-time Log Streaming to 3rd party SIEM/SOAR systems. Scheduled reports

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

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	Gareth Lockwood
Position	VP of Product
Date	24/10/23
Signature