Appropriate Monitoring for Schools

June 2022

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	Forcepoint, LLC
Address	10900-A Stonelake Blvd. Quarry Oaks 1, Ste. 350 Austin, TX 78759
Contact details	
Monitoring System	
Date of assessment	

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		Can be found: https://www.iwf.org.uk/membership/our-members/
• Utilisation of IWF URL list for the attempted access of known child abuse images		The IWF URL list is included into Forcepoint's URL Database which is the basis of the filtering provided by Forcepoint
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Forcepoint includes the CITRU URL list into Forcepoint's URL database

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		Yes. Forcepoint includes a content stripping options that makes it possible to specify that content in particular scripting languages (ActiveX, JavaScript, or VB Script) be stripped from incoming web pages. If content stripping is enabled, all content in the specified scripting languages is removed. Content is removed only after the advanced analysis options have categorized the site and Filtering Service has determined which policy applies.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Yes. Please see response above.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Yes. Please see response above.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Yes. Please see response above.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Yes. Please see response above.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Yes. Please see response above.
Pornography	displays sexual acts or explicit images		Yes. Please see response above.
Self Harm	promotes or displays deliberate self harm		Yes. Please see response above.
Suicide	Suggest the user is considering suicide		Yes. Please see response above.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Yes. Please see response above.

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

All customer events and logs are sent to the restricted access database at both customer selected data centers. Security logs are aggregated to a centralized logging server with restricted access . Additionally, customers can sign up for Tech alerts and be emailed about all pertinent information, i.e. Cloud infrastructure maintenance, new releases, etc.

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

Forcepoint includes a content stripping options that makes it possible to specify that content in particular scripting languages (ActiveX, JavaScript, or VB Script) be stripped from incoming web pages. If content stripping is enabled, all content in the specified scripting languages is removed. Content is removed only after the advanced analysis options have categorized the site and Filtering Service has determined which policy applies.

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		Yes
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Forcepoint provides “Tech Alerts” that will automatically notify subscribed customers, as the person listed in our systems as a point of contact anytime Forcepoint issues new releases, critical hotfixes, or other important technical information. Customers

		have the ability to also self-report system errors/anomalies through the myForcepoint portal.
• 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		Forcepoint solution allows for different device profiles to be deployed, which provide varying levels of control. Corporate- and education-owned devices could have profiles which provide full device control that includes MDM controls (password and device functionality), application controls, and web security. BYOD devices can have a different profile which may simply provide web filtering and security, and limit access to approved applications.
• 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		Customer generated audit data is retained for 30 days. Reporting data is retained for 30-90 days depending on product/customer configuration. Backend system audit retention (not customer generated data) 365 days. When a customer has left, the service configuration and user accounts are retained to facilitate returns. Where requested, this data can be purged.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Yes
• Flexibility – schools ability to amend (add or remove) keywords easily		Yes
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Yes
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		All users should be made aware that their online activity is being monitored.
• Multiple language support – the ability for the system to manage relevant languages?		Yes

• 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 generated via email or "Tech Alert". You can define when you want to trigger alerts and whether the alerts should be sent to the syslog or emailed to an administrator. If an alert is to be sent by email, you can define the sender, recipient(s), subject, and mail server. Our solution allows for dynamic actions.
• 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.		All remote sessions have to be agreed upon by Customer Employees and they are prompted to accept remote sessions. Remote session times are logged in support cases as proof that a meeting occurred within Forcepoint's CRM system.
• Reporting – how alerts are recorded within the system?		Every detection will trigger an incident. Where a security incident has been reported the Information Security Manager will complete the following: • Log the incident, recording the incident details and subsequent remedial activities • Identify and complete corrective actions • Where possible identify and remove the cause of the incident • Where possible identify and complete actions to prevent recurrence • Review the effectiveness of preventative actions
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		Yes

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

Forcepoint delivers the best content security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market and small organizations around the world, many being educational institutions. Several customer video case studies have been done. You can find them by the various products at https://www.forcepoint.com/resources/case-studies

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	Adam Johnson
Position	Distribution Manager
Date	07/10/2022
Signature	A.Johnson