Appropriate Monitoring for Schools

June 2018

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	
Address	
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		
● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		

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		
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		
Pornography	displays sexual acts or explicit images		
Self Harm	promotes or displays deliberate self harm		
Suicide	Suggest the user is considering suicide		
Violence	Displays or promotes the use of physical force intended to hurt or kill		

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

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

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		
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		
• 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		
• Data retention –what data is stored, where is it (physically) stored and for how long		
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		
• Flexibility – schools ability to amend (add or remove) keywords easily		
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		
• Multiple language support – the ability for the system to manage relevant 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?		
• Reporting – how alerts are recorded within the system?		

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	
Position	
Date	
Signature	