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	Smoothwall
Address	Avalon, 1 Savannah Way, Leeds, LS10 1AB, United Kingdom
Contact details	08701999500
Monitoring System	RADAR
Date of assessment	01/10/18

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	🟩	Smoothwall are IWF members, and where appropriate, use IWF material to aid monitoring alerts
● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Smoothwall work with CITRU to improve the accuracy of our PREVENT alerting

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	🟩	RADAR contains a variety of Safeguarding themes which pick up illegal content, including a theme specifically aimed at PREVENT.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	Bullying takes many forms, and RADAR can pick up bullying content in the "Racism and Violence" theme as well as others targeted at more general behaviour issues.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet	🟩	The "Predators and Strangers" theme is specifically designed to pick up this type of activity.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	The Racism and Violence theme picks up a variety of discriminatory terms, whilst the "Acronyms" theme will pick up attempts to hide discriminatory language
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	This is covered entirely by the "Drugs and Addiction" theme
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	As previously described, this is covered by a PREVENT specific

		🟩	theme along with overlap from other areas
Pornography	displays sexual acts or explicit images	🟩	The “Pornographic Content” theme is designed to pick up this activity. Smoothwall suggest this is augmented by high quality web filtering.
Self Harm	promotes or displays deliberate self harm	🟩	The “Suicide and Health” theme will pick up suicidal ideation, and self harm
Suicide	Suggest the user is considering suicide	🟩	The “Suicide and Health” theme will pick up suicidal ideation, and self harm
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Violence will be picked up by the “Racism and Violence” theme

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

RADAR’s themes are constantly being revised. Since becoming part of the Smoothwall family, RADAR benefits from Smoothwall’s Digital Safety Analysis team. Over the coming months, we can expect to see new themes, as well as improvements to existing work. Theme content is rated from 1-5 to ensure the highest priority incidents can be alerted as soon as possible.

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

RADAR is generally not used in a blocking context. In order to avoid over-alerting, a number of suppression rules are used to prevent inadvertently tripping the analysis engine. Alerts are combined in the RADAR portal such that it is easy for administrators to sort false positives.

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	🟩	RADAR can be customised by user or machine group, and alert accordingly
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	Alerts in RADAR are managed by the School. For a managed

	🟩	safeguarding service, Smoothwall suggest the Visigo product.
• 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	🟧	BYOD monitoring is not advised with RADAR client software – students' own devices are not often well secured enough to prevent removal, or properly identify the user. Smoothwall suggest using web filtering to monitor unmanaged devices.
• Data retention –what data is stored, where is it (physically) stored and for how long	🟩	Data is stored in a UK based Microsoft Azure data centre. Data retention is for 1 year
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	A software install is required. Windows, macOS, Chromebook and iOS are supported.
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	Schools are able to exclude keywords
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	RADAR is available as a multi-tenant solution on request.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	RADAR is capable of displaying an AUP to students. In addition, Smoothwall offers guidance around best practice.
• Multiple language support – the ability for the system to manage relevant languages?	🟩	RADAR currently supports English and Arabic, this range will be expanded during 2019
• 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 prioritised based on their severity – grading is a combination of RADAR's inbuilt grades, and School input grading
• Reporting – how alerts are recorded within the system?	🟩	Alerts are recorded within the RADAR portal. A full reporting suite is available as well as a r~~R~~eal-time dashboard.

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

RADAR is specifically designed to be easy-to-use and intuitive. This ensures that the software can be used by the entire staff in order to ensure that the school’s online safeguarding responsibility is fulfilled.

RADAR's Pre-Grading feature automatically assigns a level of risk to each instance of captured activity radically reducing the amount of time spent on assessing activity and ensuring that instances of risk are easily identified.

Automatic reporting, alerts and a highly-visual user interface ensure that staff can instantaneously identify potential incidents of risk allowing early intervention and escalation where necessary.

An upgrade path to Smoothwall Visigo offers a managed safeguarding alert service for schools with changing requirements.

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	Douglas Hanley
Position	CTO
Date	01/10/2018
Signature	Douglas Hanley