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	0870 1999 500
Monitoring System	Visigo
Date of assessment	01/10/2018

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 is an IWF member, 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		There are 3 Visigo themes that cover this requirement – a specific theme on Terrorism, a specific theme on CAI and an additional theme on Cyber Crime. Other criminal activity would be classed as "General Risk".
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		The "CyberBullying" 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		Visigo includes 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		Visigo's Cyberbullying 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” by Visigo.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Visigo has a “Terrorism” theme designed entirely for detection of terror and extremism content.
Pornography	displays sexual acts or explicit images		Visigo’s “Cybersexer” 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 Visigo’s “Vulnerable User” theme. If a risk to life is suspected, the DSL will receive a phone call straight away – 24x7x365.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Violent material is likely to come under a General Risk category, but depending on the target of any violence, could be classified as Terrorism or Bullying.

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

Visigo 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.

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

Visigo is not a blocking technology – rather it monitors the user and carefully builds a picture of their online and offline activities on all their managed devices. Over alerting is minimal due to the human moderation component at the heart of the Visigo service.

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		Visigo does not explicitly differentiate between users in an organisation, however an organisation will be provided a profile based on their mix of users. This will alter the alerting received by a DSL, but ultimately the classification which occurs is unchanged – this is because a user's age is not necessarily an indication of maturity or risk.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Alerts are managed via the human moderation team, who apply a severity rating before either emailing or phoning through an alert to the Safeguarding team. Each alert is described with a paragraph of text written by the moderators.
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e. 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 Visigo client software – students' own devices are not often well secured enough to prevent removal, or properly identify the user. User identity is core to Visigo's capabilities in building a picture of activity over time. 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 retained for 15 months and is stored in a UK Datacentre operated by Microsoft to the highest security standards.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Visigo's device software supports managed Windows, macOS and Chromebook devices.
• Flexibility – schools ability to amend (add or remove) keywords easily		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 managed by professional analysts.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Visigo allows users who manage more than one organisation to easily view data and manage access across their entire estate.
• 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 Visigo's monitoring
• Multiple language support – the ability for the system to manage relevant languages?		Visigo monitoring is used across the UK and supports capture of data in languages common to UK Schools.
• 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
• Reporting – how alerts are recorded within the system?		Alerts are recorded separately to captured information. All alerts are available in the portal and can be searched, linked through to associated screen captures.

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

The Visigo solution from Smoothwall allows schools and colleges the opportunity to work with a single provider to meet their Appropriate Filtering and Appropriate Monitoring expectations as set out in “Keeping Children Safe In Education”. The Visigo solution helps schools reduce the costs associated with online monitoring and increase the effectiveness of their Safeguarding activities. Additionally, integrations with a popular Safeguarding reporting tool are available.

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