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	Netsweeper
Address	Suite 125-126 Pure Offices, 4100 Park Approach Thorpe Park, Leeds United Kingdom LS15 8GB
Contact details	Nick levey
Monitoring System	Onguard
Date of assessment	10/06/2023

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		We are IWF member
• Utilisation of IWF URL list for the attempted access of known child abuse images		We integrate this list into our products along with several others
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		We integrate this list
• Confirm that monitoring for illegal content cannot be disabled by the school		This can be deployed so that it is unremovable

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		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Gambling	Enables gambling		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Pornography	displays sexual acts or explicit images		Netsweeper uses dynamic content analysis to categories , this and many other content types.

Self Harm	promotes or displays deliberate self harm		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Suicide	Suggest the user is considering suicide		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper uses dynamic content analysis to categories , this and many other content types.

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

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		Monitoring is broken down into various categories and and priority levels to allow the school to take a gradiated response based on age or vulnerability
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		A managed service is provided , however schools can still manage their own alerts of so desired
• 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 changes as logged and auditable. As are all other aspects of usage
• 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		Schools can choose to monitor BYOD devices. How this is done is dependant on the schools policy and attitude to risk
• 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		All data is stored in the UK. Data retention is definable by the customer.
• Devices – if software is required to be installed on devices, the monitoring system should be		Safeguarding functionality is available for windows, mac,

clear about the devices (and operating systems) it covers		chromebook, ios and android.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		Keyword lists can be amended for web based content
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		The system is multitenant and allows for this level of control
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Guidance can br provided but each school must make their own decisions
• Multiple language support – the ability for the system to manage relevant languages?		Multiple languages are supported
• 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?		All alerts are broken down into both subject and prioritisation categories, instant alerting varies based on the severity of the incident
• 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.		Netsweeper offers remote monitoring on various SLA's
• Reporting – how alerts are recorded within the system?		Alerts are recorded within the system itself and logged , they can then be exported if required
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		Done using specialist lists provided by various agencies. This includes IWF and CAIC

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.

Netsweeper provides pro active monitoring support with an inhouse team of UK based monitoring experts. Our team members are specifically selected for safeguarding skillsets and go through specific training form recognised external providers.

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

Netsweeper provides filtering , safeguarding and monitoring products together with training packages around safeguarding and technology

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	Nick Levey
Position	Regional Director
Date	15/06/23
Signature