

# Appropriate Monitoring for Schools

June 2020



## 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](http://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](mailto: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 Inc.
Address	Suite 125-126, 4100 Park Approach, Thorpe Park, Leeds, LS15 8GB, United Kingdom
Contact details	Product Manager: Chris Garstin ( <a href="mailto:chris.garstin@netsweeper.com">chris.garstin@netsweeper.com</a> )
Monitoring System	Netsweeper for Education
Date of assessment	2020-06-04

### 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.		Netsweeper <b>is a member of the IWF</b> in good standing, and actively works with the IWF to find and block access to CSAM material.
and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Netsweeper for Education includes the <b>IWF list</b> and can block all access to the URLs on the list.
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Netsweeper for Education includes the <b>CTIRU list</b> of terrorist content and can block all access to the URLs on the list.

## 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 for Education with nMonitor technology includes the “ <b>nMonitor Violence</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Illegal</b> ” themed content.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Violence</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Bullying</b> ” themed content.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Predators</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Child Sexual Exploitation</b> ” themed content.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Violence</b> ” category for blocking.  We are working to further enhance our monitoring categories to address these themes.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Addiction</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Drugs / Substance abuse</b> ” themed content.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Prevent</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Extremism</b> ” themed content.
Pornography	displays sexual acts or explicit images		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Pornography</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Pornography</b> ” themed content.
Self Harm	promotes or displays deliberate self harm		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Suicide</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Self-Harm</b> ” themed content.
Suicide	Suggest the user is considering suicide		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Suicide</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Suicide</b> ” themed content.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper for Education with nMonitor technology includes the “ <b>nMonitor Violence</b> ” category for blocking.  This category meets the requirement for blocking “ <b>Violence</b> ” themed content.

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

In addition to the categories above for nMonitor, there are many additional categories that can be utilised to analyse student behaviour. These categories are scanned in multiple languages as well.

Combining the nMonitor technology with Netsweeper for Education’s comprehensive web filtering platform, a complete picture of student activity can be generated from one source.

Netsweeper also has a Content Support Team as well, focused on reviewing both web filtering and nMonitor incidents and inaccuracies. This team will review any inaccuracies, and continually train the CNS and nMonitor AI systems.

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

Netsweeper nMonitor technology is constantly being refined by Netsweeper to ensure detection is within reasonable limits of over-blocking. Importantly, the nMonitor solution does not block at all, but only scans activity and raises alerts to school stakeholders, such as the DSL.

It's important that false positives are limited without affecting the true positives rate, and Netsweeper is working with various organisations, and well as beta program customers, to ensure that nMonitor is constantly improving its ability to help at-risk students.

### 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		Netsweeper for Education with nMonitor technology enables alerting to be tailored to the unique needs fo each school.
Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Alerts can be configured to trigger based on theme and priority level. Alerts are emailed to school administrators or DSLs for further action.
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		<p>Netsweeper nMonitor technology can be deployed to BYOD devices but cautions that this may have limited impact.</p> <p>BYOD devices cannot be “locked-down” the same as school-owned assets, meaning a student can remove any software installed by the school.</p> <p>Netsweeper’s URL filtering also contributed to student safeguarding and has a number of method for handling BYOD devices.</p>
Data retention –what data is stored, where is it (physically) stored and for how long		<p>The Netsweeper for Education with nMonitor technology includes a highly configurable logging and reporting system that can be adjusted to meet regional requirements with respect to data retention.</p> <p>Netsweeper recommends storing log file data for 3 years or more.</p>

Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Windows, Mac/OSx, Chrome  Where possible, this will be extended to iOS and Android, but not at this time.
Flexibility – schools ability to amend (add or remove) keywords easily		Netsweeper’s search keywords functionality enables system operators to easily make changes to words that Netsweeper is scanning for.
Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Netsweeper for Education includes comprehensive multi-tenant capabilities and is highly scalable to support many schools operating on a single platform. Each school is “siloeed” within their own operational environment.
Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Netsweeper’s deny page framework and captive portal functionality enable operators to present informative pages to their end users, informing them of monitoring activity.
Multiple language support – the ability for the system to manage relevant languages?		Netsweeper for Education with nMonitor technology includes multi-language support for categorisation and well as the management interface.
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?		Netsweeper for Education with nMonitor technology includes a powerful reporting/alerting engine that can be tuned to the needs of each school. Report alerts are configured to trigger to at a set interval, and when triggered can email the DSL to inform them of incidents needing review.
Reporting – how alerts are recorded within the system?		Netsweeper for Education with nMonitor technology includes a fully customisable reporting framework. The reporting framework uses the URL Request Log files, which contain information on every URL request and nMonitor incident that the Netsweeper solution processes.

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

Netsweeper’s nMonitor technology is relatively new and evolving. Netsweeper is working closely with child protection organizations, as well as our customers through the nMonitor beta program, to validate that nMonitor provides industry leading student protection. Netsweeper is also establishing the ongoing processes to continually validate the effectiveness of the nMonitor technology, and continually improve its effectiveness.

By combining the nMonitor technology into the overall Netsweeper for Education solution, student safeguarding can be accomplished through a single platform, from a company that shares the same mission, and at a reasonable cost.

## 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	Chris Garstin
Position	Product Manager
Date	2020-06-04
Signature	