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) 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	NetSupport Limited
Address	NetSupport House, Market Deeping, Peterborough, PE6 8NE
Contact details	Al Kingsley
Monitoring System	NetSupport DNA for Education
Date of assessment	30th June 2020

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		NetSupport has been a member of the IWF since January 2016. The IWF keyword list is integrated into our own Safeguarding keyword library. https://www.iwf.org.uk/member/netsupport-software
• Utilisation of IWF Hash list to identify the storage or transmission of known child abuse images		Not utilised in our solution.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		NetSupport has worked with CTIRU since Autumn 2016 and confirm that the Police Assessed List of Unlawful Terrorist Content (URL Blacklist) is integrated into our monitoring software.

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		Integrated Grooming/Child abuse (IWF Keywords) and Radicalisation keyword libraries monitor all content typed, copied or searched for within any application that would suggest a young person is vulnerable to exploitation in these areas or displaying extremist views. Our lists are supplemented and kept current by our teams own ongoing research and in partnership with relevant charities and local community organisations. Customers also have the option to add their own custom keywords to ensure specific local issues are managed effectively.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Bullying keyword library monitors all content typed, copied or searched for within any application to help identify children that may be engaging in bullying behaviour or be the target of bullies. Incorporates

			street slang associated with gang culture.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Grooming keyword library (IWF Keywords) monitors all content typed, copied or searched for within any application to identify and report on any inappropriate behaviour across the school site or communications with external parties/strangers.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Racism and Homophobia keyword libraries monitor all content typed, copied or searched for within any application in order to highlight any discriminatory behaviour.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Drugs keyword library monitors all content typed, copied or searched for within any application that relates to the use or purchase of drugs/alcohol and other harmful substances. Slang variants of drug terms and smart/study drugs also included.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Radicalisation keyword library monitors all content typed, copied or searched for within any application that suggests an interest in or the promotion of any form of extremism, extreme political views or references to weapons. Linked to Prevent Duty guidance.
Pornography	displays sexual acts or explicit images		Adult keyword library monitors all content typed, copied or searched for within any application that suggests an inappropriate interest in adult content or the sharing of such content. Acronyms, abbreviations and common slang also included.
Self Harm	promotes or displays deliberate self harm		Self-Harm and Eating Disorders keyword library monitors all content typed, copied or searched for within any application that suggests the young person is vulnerable in these areas. Our ongoing research and work with specialist partners and charitable organisations ensure our libraries are current across all areas of

			mental health awareness, online crazes and addictions.
Suicide	Suggest the user is considering suicide		Suicide keyword library monitors all content typed, copied or searched for within any application that suggests the young person is considering suicide or showing signs of depression. Includes information relating to pro-suicide websites and online games that promote suicide. Our ongoing research and work with specialist partners and charitable organisations ensure our libraries are current across all areas of mental health awareness.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Covered within the Bullying and Radicalisation keyword libraries, monitors all content typed, copied or searched for within any application that suggests threatening behaviour or acts of violence and extremism. Supplemented with terms and slang relating to Honour Based Violence (HBV), Female Genital Mutilation (FGM) and gang culture.

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

To offer schools this tool to help effectively safeguard their students, NetSupport works with internationally operating organisation, the Internet Watch Foundation, the Counter Terrorism Internet Referral Unit (CTIRU) and collaborates closely with its local authority, school safeguarding leads and local schools as well as specialist charities to ensure the keywords, phrases and detection signatures supporting NetSupport DNA's technology are as comprehensive and relevant as possible and include common misspellings, slang and chat/text speak.

Ongoing research and collaboration with our Safeguarding partners combined with customer feedback ensures each regular update of NetSupport's keyword libraries cover the latest trends across all areas of Child Safeguarding and Online Safety.

Working with Local Safeguarding leads and community representatives, the technology also includes multi-lingual phrases to support many of the most common languages spoken in schools and extends to Welsh and Scottish/Gaelic.

Each keyword/phrase is supported by an English definition to aid the customers understanding to ensure informed decisions can be taken when localised phrases are triggered. Extending the language set is a key part of the long-term evolution of NetSupport's solution as we respond to the ever-changing multi-cultural nature of schools.

To ensure local trends are managed effectively, individual schools and multi-academy trusts can add their own custom terms and slang and use NetSupport DNA's flexible user-profiling options to target alerts to the relevant staff members.

A variety of real-time alerting methods ensure staff members can immediately identify and react to safeguarding events in a timely and appropriate manner. The software's 'welcome' dashboard provides an instant statistical analysis of matched phrases, filtered by date, severity and the number that include supporting evidence. (Severity levels allocated to safeguarding keywords dictate the outcome on matching: from a simple recording of the activity in the system, through to an instant alert or screen capture.)

The software's main eSafety component provides the specific details of the triggered event such as student logon ID, the PC used and the time it was triggered, and for determining context, what was typed or searched for and the application used. You can then print, save, email or take a screen grab of the results to forward to a colleague to follow up on – or, alternatively, if not a real concern, simply mark the event as a false alarm. A handy word cloud provides further insight into what safeguarding issues are trending at your school, enabling you to monitor and intervene where needed, even drilling down to see trends by year group for any given period of time.

The software's contextual intelligence-based Risk Index automatically flags high-risk events and vulnerable students, based on sophisticated contextual AI risk analysis. It assesses the context and history of a child's activities – from the devices used, time of day, and websites visited (including previous alerts they may have triggered) – and, from this information, creates a numerical risk index. A high-risk index could result if a child has repeatedly researched a safeguarding topic (e.g. suicide) out of hours, in an unmonitored setting such as the library. A lower index rating could result from a student searching a lower risk keyword in a local application during school hours that may have been used for curriculum topics.

All the monitoring and assessment of these alerts is done locally by the school (no third-party services are required) and so the data is fully secure. This allows staff to focus on high-risk alerts (where there is more likely to be a genuine risk) and allows them to apply their professional judgement.

As well as the software's desktop User Console, a secure, Azure-hosted 'Cloud' based Safeguarding Console is also provided, designed to help Safeguarding staff access alerts on the go.

The 'Report a Concern' tool allows students to proactively report issues to a nominated member of staff, encouraging dialogue when support is needed. Concerns, supporting documents and history of steps are all securely recorded. NetSupport DNA includes all the reports and evidence to demonstrate on inspection the effectiveness of your safeguarding and Prevent policies. Concerns can be reported via an 'Agent' installed on each school desktop/mobile device or the software also offers the facility for customers to add a custom 'Report a Concern' button to the school's website allowing 24/7 access to students. Teachers also have the capability to log a Concern on behalf of students.

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

NetSupport DNA has a number of safeguarding features that allow a school to monitor and be alerted of potential issues. The system allows the level of enforcement by the product to be tailored to meet their needs and can be set to exclude selected applications, adapt filtering by

time of day and more. Keyword detection thresholds can also be adjusted as required. The solution was developed with safeguarding leads to remove the overhead from IT staff of maintaining the system. It is optimised to reduce “false positives” triggers and can monitor and report data without needing alerts to be sent for every violation.

Features include:

- Keyword and Phrase Monitoring
- Providing a method for children to Report a Concern to a trusted staff member
- Internet Monitoring (and restrictions where required)
- To aid the review process, the addition of crucial supporting evidence alongside the triggered phrase, such as screen shots, screen recordings and, if appropriate, a webcam image of the person using the PC at the time, provide added context.
- The ability to disable the Webcam (if appropriate)
- A word cloud enabling schools to see trending topics, words and phrases in school.
- Safeguarding staff can flag 'at risk/vulnerable' students on the system so they can be easily identified and tracked as an extra layer of support.
- Contact details for appropriate support agencies/helplines for each safeguarding area is accessible by staff and students to ensure, if needed, professional advice can be sought at the earliest opportunity.

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		Fully configurable staff/student user profiles allow restrictions and keyword monitoring tolerances to be set at appropriate age (or year group and location) level. Profiling also extends to being able to select which teachers/staff are available for students to report concerns to. This is especially useful for schools in multi-academy trusts, who can simply select the relevant profile displaying the safeguarding contacts for their own school.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		A NetSupport DNA console operator has a mix of pro-active alerting options at their disposal to ensure triggered Safeguarding events are managed and responded

		to in a timely and effective manner. Custom user profiles also allow schools, whether individual or multi-site, to direct alerts and send automated emails to the appropriate staff member. The Home screen dashboard provides a real-time summary of current network activity including a statistical breakdown of triggered Safeguarding keywords categorised by severity and the number that include supporting evidence in the form of screenshots and screen recordings. The number of reported student concerns that require a response is also instantly visible on the dashboard. The main eSafety component displays an innovative word cloud showing the triggered keywords in visual form. This is particularly useful for quickly highlighting trending topics across the school to help you put incidents into a broader context. You can quickly switch views to see the data in graph format along with a breakdown of keywords by category. For added context, you can drill-down further and see the PC name where the alert was triggered along with the Logged in username, application used and the matched phrase along with the

		sentence typed that contains the phrase. The Severity level assigned to each keyword controls the outcome on matching: from a simple recording of the activity, through to capturing a screenshot or a video of the devices screen. It can also, if enabled by the school, capture an image of the user via the webcam - so you know the full background to the event. The triggered event can also be exported to PDF format making it easier to share with school staff. Triggered phrases can also be marked as false alarms. NetSupport DNA also features a dedicated Alerting module that automatically notifies operators when changes occur across the school network - and this includes triggered keyword alerts. Alert notifications can be directed to specified email recipients and/or active console users (on a per alert basis, so the nature of the alert may dictate which operators are notified). In addition, outstanding alerts are identified against matching PCs on the main hierarchy tree view. Once alerts have been identified, notes can be added by an operator. A full history of

		all alerts is accessible from the History feature.
• 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		The system will detect other PCs, Laptops and devices that join the network and an Agent can be dynamically deployed to the device to track inventory and activity monitoring. The installed Agent can continually monitor device activity beyond the school hours and location if required.
• Data retention –what data is stored, where is it (physically) stored and for how long		Keywords matched, PC ID, logged on user and time of day. All data is stored in an encrypted database with an audit history recording all views of the data. A 'Database Maintenance' facility allows customers to choose when to purge the system of historical data and there are options available that enable a permanent record of triggered phrases to be held if required for inspection. For example, export to PDF. When the system is used across schools that are linked (e.g. multi-academy trusts), on an operational level, an individual school can see its own data, while that of other schools is unavailable. At a higher level, the data across all of the separate sites can be seen and analysed as a consolidated report.

• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		The system pre-requisites, supported platforms and install instructions applicable to each device (Desktop and Mobile) are fully outlined in the systems built-in help, online user guides, website and on app stores.
• Flexibility – schools ability to amend (add or remove) keywords easily		Custom keyword database with option to add terms, and import/export terms shared with peers.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		When NetSupport DNA is used across schools that are linked (e.g. multi-academy trust), on an operational level, the setting of profiled user-views allows an individual school to see its own data, while that of other schools is unavailable. At a higher level, the data across all of the separate sites can be seen and analysed as a consolidated report.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Product can deliver, display and track school acceptable use policies. Full deployment and delivery guidance included in getting started guide.
• Multiple language support – the ability for the system to manage relevant languages?		Solution is available in a number of languages and keyword libraries are now available for many common languages spoken in UK schools and extends to Welsh and Scottish/Gaelic. Introduction of additional languages is ongoing as we respond to the evolving multi-cultural nature of most 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?		All alerts triggered based on keyword and category can be prioritised from Low, Medium, High or Critical. Level of priority dictates if alerts or emails sent, and what information is captured. Keywords in the Suicide and Self-Harm libraries are flagged as High priority by default. In addition, the software's in-built contextual intelligence-based 'Risk Index' creates a numerical risk index for each event based on sophisticated contextual AI risk analysis. This allows staff to view high-risk events and vulnerable students with ease.
• Reporting – how alerts are recorded within the system?		The system offers a wealth of reporting options and views to allow Safeguarding Users to review alerts - for both triggered keywords and concerns reported by vulnerable students. Pre-prepared on screen reports showing all alerts by category and keyword and newly received Student Concerns. Dynamic word cloud showing data captured by dept, year group and more. Pre Supplied Crystal reports for management reporting of all violations in detail or summary format. A Query Tool

		that allows users to define custom views. Safeguarding Users can also see a history of concerns reported by a specific student, laid out in calendar format, giving them the ability to review the pattern and detail of issues raised over time.

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

NetSupport DNA Education suite also includes tools to monitor and interact with students. These include :
Report a Concern – a child can report a concern (along with supporting screenshot or document to evidence) from any PC using the NetSupport DNA app, this is delivered directly to prenominated staff where concerns can be tracked and managed centrally in the system. For out-of-hours use or when a school device isn't readily available to vulnerable students, schools also have the option to embed a bespoke 'Report a Concern' button, linked to their central DNA Console, on the school website to offer 24/7 reporting capabilities.

Safeguarding staff can flag 'at risk/vulnerable' students on the system so they can be easily identified and tracked as an extra layer of support.

Safeguarding resources – NetSupport DNA provides a custom list of safeguarding resources (websites and Helplines) for students to access from any PC .

Option to disable the webcam on school devices provides an additional layer of safety and security.

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	Alastair Kingsley
Position	Managing Director
Date	30th June 2020
Signature