

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	NetSupport Limited
Address	NetSupport House, Market Deeping, Peterborough, PE6 8NE
Contact details	01778 382270 / support@netsupportsoftware.com
Monitoring System	NetSupport DNA for Education - School IT asset management & safeguarding
Date of assessment	25 th May 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
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Utilisation of IWF URL list for the attempted access of known child abuse images 		Not currently used.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Confirm that monitoring for illegal content cannot be disabled by the school 		Schools do have the option to disable monitoring in the DNA Administrator Console but system admins can avoid inadvertent disabling of the software by colleagues by applying appropriate permissions to each console user role.

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 (covers areas such as terrorism, supremacy and Incel movement). Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. Our lists are supplemented and kept current by our teams own ongoing research and in

			partnership with relevant charities and local community organisations.
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 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. The integrated IWF library is supplemented with terms covering subjects such as Peer Abuse/coercion.
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. Terms relating to County Lines 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.
Gambling	Enables gambling		Gambling keyword category monitors all content typed, copied or searched for that

			suggests participation in or addiction to any form of gambling, online betting apps or otherwise.
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		Separate Self-Harm, Eating Disorders and Gambling keyword libraries monitor 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. Keywords in this category are automatically assigned 'Urgent' status in order to raise the profile of alerts to Safeguarding leads.
Suicide	Suggest the user is considering suicide		Suicide and Wellbeing 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. Keywords in this category are automatically assigned 'Urgent' status in order to raise the profile of alerts to Safeguarding leads.
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,

			<p>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.</p>
--	--	--	--

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/video 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 add progress notes to each incident, 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.

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.

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.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> 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 		<p>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</p>

		<p>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.</p>
<ul style="list-style-type: none"> Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided 		<p>A NetSupport DNA console operator has a mix of pro-active alerting options at their disposal to ensure Safeguarding events are managed and responded to in a timely and effective manner.</p> <p>Custom user profiles also allow schools, whether individual or multi-site, to direct alerts and send automated emails to the appropriate staff member.</p> <p>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.</p> <p>The number of reported student concerns that require a response is also instantly visible on the dashboard.</p> <p>An innovative word cloud shows the triggered keywords in visual form. This is</p>

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. The triggered event can also be exported to PDF 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

		<p>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.</p>
<ul style="list-style-type: none"> 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. 		<p>NetSupport DNA provides an Audit Log, which allows you to keep track of actions that users have taken within the NetSupport DNA Console. Console activities such as, when users have logged in and out of the Console, when components have been enabled or disabled, AUP documents created and assigned and any changes to the component settings are recorded.</p>
<ul style="list-style-type: none"> 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>The school is in full control of which devices are monitored. NetSupport DNA’s remote Agent application needs to be installed on devices before they can be monitored.</p> <p>In a BYOD scenario, the system will detect unrecognised devices (tablets, laptops etc) that join the network and the Agent can be dynamically deployed to the device.</p>

		<p>The installed Agent can continue gathering data beyond the school hours and location if required.</p>
<ul style="list-style-type: none"> • 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 		<p>As an on-premise application, all data is stored within the school infrastructure and is therefore retained inline with each sites local policy. Data captured includes Keywords matched along with the PC ID, logged on username and date/time. Higher priority keyword triggers will also capture a screenshot/video of the event. Reviewers notes are also attached to the record. In addition, details of reported student concerns are held.</p> <p>All data is stored in an encrypted database with an audit history recording all views of the data.</p> <p>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.</p> <p>When the system is used across schools that are linked (e.g. multi-academy trusts), on an</p>

		<p>operational level, an individual school can see its own data, while that of other schools is unavailable.</p> <p>At a higher level, the data across all of the separate sites can be seen and analysed as a consolidated report.</p>
<ul style="list-style-type: none"> • Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers 		<p>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.</p>
<ul style="list-style-type: none"> • Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy 		<p>Custom keyword database with option to add terms, and import/export terms shared with peers.</p>
<ul style="list-style-type: none"> • Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>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.</p>
<ul style="list-style-type: none"> • Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools? 		<p>Product can deliver, display and track school acceptable use policies. Full deployment and delivery guidance included in getting started guide.</p>
<ul style="list-style-type: none"> • Multiple language support – the ability for the system to manage relevant languages? 		<p>Solution is available in a number of languages</p>

		<p>and keyword libraries are now available for many common languages spoken in UK schools and extends to Welsh and Scottish/Gaelic.</p> <p>Introduction of additional languages is ongoing as we respond to the evolving multi-cultural nature of most schools.</p>
<ul style="list-style-type: none"> • 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? 		<p>All alerts triggered based on keyword and category can be prioritised from Low, Medium, High or Critical.</p> <p>Level of priority dictates if alerts or emails sent, and what information is captured.</p> <p>Keywords in the Suicide and Self-Harm libraries are flagged as High priority by default.</p> <p>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.</p>
<ul style="list-style-type: none"> • 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. 		<p>NetSupport DNA is an on-premise tool and as such is not designed for monitoring away from the school site. However, if a BYOD device has the Agent software installed, the device will still monitor</p>

		<p>for phrase matches but the recorded data will not be sent to the DNA Admin Console until the device reconnects to the school network.</p>
<ul style="list-style-type: none"> Reporting – how alerts are recorded within the system? 		<p>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.</p> <p>Pre-prepared on-screen reports showing all alerts by category and keyword and newly received Student Concerns.</p> <p>Dynamic word cloud showing data captured by dept, year group and more.</p> <p>A Query Tool that allows users to define custom views.</p> <p>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.</p>
<ul style="list-style-type: none"> Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash) 		<p>Image hashing isn't employed as such. NetSupport DNA is monitoring for typed or searched keywords but as mentioned, higher priority triggers do include supporting screenshots and recordings to aid the review process.</p>

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.

NetSupport DNA delivers a number of tools to allow pro-active monitoring. The ability for admins to create 'safeguarding groups' (eg age related groups or ease of identification of particularly vulnerable students), create automated custom email alerts for all or specific risks, assigned to the required member of the safeguarding team. Additional emails triggered when events are reassigned to colleagues.

Contextual intelligence risk index score based on a number of factors to highlight the urgency of triggered events – source of trigger (typed or web search), number of occurrences of similar incidents for the same students.

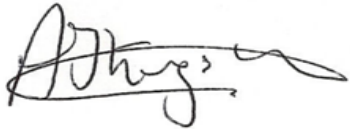
Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

For a full summary of how NetSupport products support KCSIE please refer to the following:
<https://www.netsupportsoftware.com/kcsie/>

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	CEO, NetSupport Group
Date	25 th May 2023
Signature	

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	NetSupport Limited
Address	NetSupport House, Market Deeping, Peterborough, PE6 8NE
Contact details	01778 382270 / support@classroom.cloud
Monitoring System	classroom.cloud by NetSupport – cloud based safeguarding, IT management & classroom instruction
Date of assessment	25 th May 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
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Utilisation of IWF URL list for the attempted access of known child abuse images 		Not currently utilised.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Confirm that monitoring for illegal content cannot be disabled by the school 		Schools do have the option to disable monitoring in the classroom.cloud Administrators cloud based web portal if required but the main system admin can avoid inadvertent disabling of the software by colleagues by applying appropriate permissions to each portal user role.

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 (covers areas such as terrorism, supremacy and Incel movement). Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. Our lists are supplemented

			and kept current by our teams own ongoing research and in partnership with relevant charities and local community organisations.
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 and topics such as coercive control and misogyny.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Grooming keyword library 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. The integrated IWF library is supplemented with terms covering subjects such as Peer Abuse/coercion.
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. Terms relating to County Lines 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.

Gambling	Enables gambling		Gambling keyword category monitors all content typed, copied or searched for that suggests participation in or addiction to any form of gambling, online betting apps or otherwise.
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		Separate Self-Harm, Eating Disorders and Gambling keyword libraries monitor 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. Keywords in this category are automatically assigned 'Urgent' status in order to raise the profile of alerts to Safeguarding leads.
Suicide	Suggest the user is considering suicide		Suicide and Wellbeing 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. Keywords in this category are automatically assigned 'Urgent' status in order to raise the profile of alerts to Safeguarding leads.

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

NetSupport works with internationally operating organisation, the Internet Watch Foundation, the Counter Terrorism Internet Referral Unit (the CTIRU filtering list is not currently integrated into classroom.cloud) 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 classroom.cloud’s technology are as comprehensive and relevant as possible and include common misspellings, slang and chat/text speak.

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, schools can add their own custom phrases and ‘opt-in’ to sharing these terms with our team for inclusion in our master library.

classroom.cloud’s Safeguarding dashboard provides an instant statistical analysis of matched phrases in a variety of formats to aid analysis – word cloud, itemised list or graph.

The displayed data can be filtered in a number of ways; by school site, date/time, category, source of the trigger (copied, typed, searched, and you can choose to configure classroom.cloud to connect to the school’s Microsoft 365 tenancy so you can monitor Teams Chats and Channels), severity and risk attached to the triggered phrase. A severity grading allocated to each keyword dictates the outcome on matching: from a simple recording of the activity in the system, through to an instant alert or screen/video capture. Targeted email alerts (based on location, category and severity) can be created to ensure the appropriate staff member is immediately notified of triggered terms.

The dashboard allows you to drill-down into the specific details of the triggered event, 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. Captured screenshots or recordings can also be viewed

alongside the phrase. You can print or export the information. If, on review, the triggered event is not a real concern, simply mark it as a false alarm.

To further aid the review process, classroom.cloud’s contextual intelligence-based Risk Index helps your school fully determine the severity of triggered events and ensures you can quickly and easily identify and support vulnerable students.

The Risk Index assesses the context and history of a student’s current activities (the device used, time of day, websites visited, and applications used) and considers them alongside any previous alerts they may have triggered. From this information, it creates a risk index number that is applied to the event. So, if a student has repeatedly researched an online safety topic (e.g. suicide) out of lesson time, a high risk index could result. A lower index rating could come from a student searching a lower risk keyword in a local application during a lesson that may have been used for curriculum topics.

Each classroom.cloud user is assigned the required access rights based on their role(s) within the academy trust or school – system admin, teacher or safeguarding user. This ensures that only appropriate staff members can review the triggered keywords.

Another strand to the Safeguarding component is the ‘Report a Concern’ tool, allowing students to proactively report issues to a nominated member of staff, encouraging dialogue when support is needed. Concern details and a history of steps are all recorded and can be exported, printed or emailed, enabling you to demonstrate on inspection the effectiveness of your safeguarding policies.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> 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 		<p>With classroom.cloud you can create ‘Safeguarding Groups’ and apply specific settings to each. For example, students in year/grade 9 or identified as vulnerable, may have different safeguarding settings to those who are in year/grade 11.</p> <p>Profiling also extends to being able to select which 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.</p>
<ul style="list-style-type: none"> Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided 		<p>Safeguarding alerts are managed solely by the school.</p>

eMail alerts can be created based on a variety of criteria (location, keyword priority and category) to ensure each staff member receives relevant notifications of keyword triggers.

The innovative word cloud shows 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.

For added context, you can drill-down further and see the PC name where the alert was triggered along with the logged in username, the source of the trigger (application, website, Teams chat etc), the risk value, and the matched phrase along with the sentence typed that contains the phrase.

All views are highly customisable, enabling the user to filter the displayed data as needed.

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.

The triggered events can also be exported to a file or printed, making them easier to share with school staff.

The number of reported student concerns that require a response

		<p>is also instantly visible on the dashboard.</p>
<ul style="list-style-type: none"> • 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. 		<p>classroom.cloud includes an Audit Log component that records any actions taken by users that may affect system configuration and stores details of any housekeeping activities Safeguarding teams may have performed.</p>
<ul style="list-style-type: none"> • 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>The school is in full control of which devices are monitored and determines, via the products Privacy Settings, the times when monitoring is live.</p> <p>Before any device can be monitored, the school will need to deploy the classroom.cloud Student (Remote Agent) application to it.</p> <p>Keyword Monitoring is supported on Windows, macOS, Apple iOS, Android (coming soon) and Chrome OS.</p>
<ul style="list-style-type: none"> • 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 		<p>Classroom.Cloud uses Microsoft Azure to provide its cloud technology. Storage is at various Azure Data Centres around the world. (Each schools classroom.cloud licence confirms the specific region.)</p> <p>At the end of a subscription or evaluation of the service, data will be retained for a 30-day period. At the end of the 30-day period, if the subscription has not been renewed or evaluation extended, then all data relating to the account will be removed.</p> <p>If an account is terminated by NetSupport then all data will be removed immediately.</p> <p>While the subscription continues to be live, historical data will be</p>

		<p>retained for a rolling 13-month period, data older than 13 months will be purged from the system.</p> <p>Information relating to triggered keywords and reported student concerns, as outlined earlier, is retained.</p>
<ul style="list-style-type: none"> • Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers 		<p>As outlined earlier, devices can only be monitored once the classroom.cloud Student software is installed. Installer pages, along with installation guides and clear sign posting of system requirements, for each supported platform are provided within the Admin Portal to ensure that the enrolment of devices into a classroom.cloud environment is a quick and simple process.</p>
<ul style="list-style-type: none"> • Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy 		<p>Schools can add their own custom keywords and opt-in to share their terms with our team for inclusion in the master library for future global updates.</p> <p>While schools cannot edit the actual keywords and descriptions supplied in the classroom.cloud library, the priority rating of any keyword can be changed, even excluded from monitoring if needed, or marked as a false alarm.</p>
<ul style="list-style-type: none"> • Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>classroom.cloud is designed for use in multi or single site environments.</p> <p>Upon creating an account, an Administrator for the whole 'organisation' (whether one site or many) is established, allowing central management of the entire classroom.cloud environment.</p>

		<p>The global Admin can then appoint individual 'Site' and 'Tech' Admins with local responsibility for overseeing the management of the school devices and user accounts relevant to that individual location. This includes assigning the appropriate access rights to teachers (for accessing their classes and using classroom.cloud's classroom management tools) and safeguarding staff with responsibility for reviewing keywords.</p> <p>Therefore, with this hierarchal approach, safeguarding alerts can be viewed and managed locally or organisation wide.</p>
<ul style="list-style-type: none"> Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools? 		<p>Schools are encouraged to have acceptable use policies in place for monitoring and classroom.cloud's AUP component allows Admins to create policies and assign them to the required user groups across the school – staff and/or students.</p> <p>Within classroom.cloud, at a global or local level, phrase monitoring can be enabled or disabled with a single click.</p> <p>Similarly, privacy settings, applied across the organisation or locally, determine when monitoring is in force.</p> <p>classroom.cloud is also highly configurable and when teachers want to connect to student devices, custom messages can be displayed on the student screens to advise that a connection has been made and when an individual student screen is being monitored.</p>

		<p>Additional help and advice in this area can be found at:</p> <p>https://classroom.cloud/privacy-by-design/</p> <p>https://classroom.cloud/data-processing-agreement/</p> <p>https://classroom.cloud/privacy/</p> <p>https://classroom.cloud/terms-of-service/</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages? 		<p>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, Scottish/Gaelic and the latest addition - Ukrainian.</p> <p>Introduction of additional languages is ongoing as we respond to the evolving multi-cultural nature of most schools.</p>
<ul style="list-style-type: none"> 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? 		<p>All alerts triggered based on keyword and category are prioritised from Low to Urgent.</p> <p>The level of priority dictates what actions take place. From a simple recording of the trigger, the sending of an email alert to the assigned reviewer, or a screen capture or recording of the incident.</p> <p>Keywords in the Suicide and Self-Harm libraries are flagged as High priority by default to ensure they are immediately visible.</p> <p>In addition, the software’s in-built contextual intelligence-based ‘Risk Index’ creates a numerical risk index for each event based on sophisticated</p>

		<p>contextual AI risk analysis. This allows staff to view high-risk events and therefore quickly identify vulnerable students with ease.</p> <p>The 'risk' score is based on a number of factors. The keyword priority, the source of the trigger (eg website search or typed into an application), was the trigger during or outside of lesson time, and the number of historical incidents attributed to the student.</p> <p>The dashboard phrase cloud, as described earlier, colour codes triggered terms to aid identification and this combines with the ability to quickly switch views to see the data in a list or graph form, filtered by urgency.</p>
<ul style="list-style-type: none"> 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. 		<p>Being a cloud based solution, classroom.cloud is the ideal platform for effective classroom management and teaching, whether everyone is together in the classroom or learning remotely at home.</p> <p>However, potential privacy issues with this model are respected.</p> <p>As such, schools can apply, globally or at individual site level, separate Privacy Settings for the general interaction with devices during lesson time and those required for safeguarding purposes.</p> <p>Settings can be applied by time of day (school hours), date (term dates), and you can restrict monitoring to just school network addresses/WiFi.</p>
<ul style="list-style-type: none"> Reporting – how alerts are recorded within the system? 		<p>The system offers a wealth of on-screen reporting options and views to allow Safeguarding</p>

		<p>Users to review alerts quickly and efficiently.</p> <p>As described previously, the dashboard is highly configurable, allowing you to filter views by category, priority, risk, device/user and more.</p> <p>The ability to quickly switch from the Phrase Cloud to a graphical representation or a detailed list, ensure maximum flexibility when reviewing the alerts.</p> <p>Clicking on a keyword trigger, username or device opens up the full review window where you can fully assess the severity of each individual alert; confirming the elements that contributed to the risk score, viewing any supporting screenshots and recordings, as well as adding progress notes and changing the status to In Progress or Completed.</p> <p>The same flexibility is also available with reported student concerns.</p>
<ul style="list-style-type: none"> • Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash) 		<p>classroom.cloud is purely monitoring for typed or searched keywords but as mentioned, depending on the priority attached to the keyword, supporting screenshots and recordings are supplied with the alert.</p>

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.

classroom.cloud delivers a number of tools to allow pro-active monitoring. The ability for admins to create 'safeguarding groups' (eg age related groups or ease of identification of particularly vulnerable students), create automated custom email alerts for all or specific risks, assigned to the required member of the safeguarding team. Additional emails triggered when events are reassigned to colleagues.

Contextual intelligence risk index score based on a number of factors to highlight the urgency of triggered events – source of trigger (typed or web search), number of occurrences of similar incidents for the same students.

Integration with 3rd party tools – CPOMS, MYCONCERN and Microsoft Tenancies for monitoring of Teams chats.

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

For a full summary of how NetSupport products support KCSIE please refer to the following:
<https://www.netsupportsoftware.com/kcsie/>

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	CEO, NetSupport Group
Date	25 th May 2023
Signature	