Appropriate Monitoring for Schools

UK Safer Internet Centre
www.saferinternet.org.uk
brought to you by SWGfL Childnet IWF

June 2021

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 they “should be doing all that they reasonably can to limit children’s exposure to the above 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.

This response includes two solutions:

Page 2

NetSupport DNA

Page 20

classroom .cloud

powered by NetSupport

NetSupport DNA for Education

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	30th June 2021

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.
● Utilisation of IWF URL list for the attempted access of known child abuse images	🟨	Not currently used.
● 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.
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.
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** 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

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.

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

Over-blocking can mean that any potential safeguarding problems are simply shifted elsewhere, so NetSupport DNA offers schools an insight into their students' online activities so that they are aware of exactly what risks students are being exposed to, as well as being able to gauge their understanding of the elements of digital citizenship. Its flexible tools ensure that checks are in place to ensure a safe environment in which to learn.

The system allows the level of enforcement by the product to be tailored to meet individual 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.

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 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. An 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 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 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 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. 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. The installed Agent can continue gathering data beyond the school hours and location if required.
● 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	🟩	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. 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	🟩	All alerts triggered based on keyword and

immediate issues. What operational procedures are in place to facilitate that process?	🟩	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.
• 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.	🟩	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 instale
• 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.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)	🟩	Image hashing isn't employed. 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.

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

The NetSupport DNA Education suite (in combination with our Classroom Management solution, NetSupport School) helps schools meet their safeguarding requirements in line with the KCSIE guidance as follows. (The relevant extracts of the guidance are provided for context):

"School and college staff are particularly important as they are in a position to identify concerns early, provide help for children, and prevent concerns from escalating."

With the help of the Keyword and Phrase monitoring tool (NetSupport DNA) and via Monitor Mode (NetSupport School), teachers can gain an insight into students' activity as they use school technology. In addition, NetSupport DNA allows teachers to document any concerns about individual students via its 'Add a concern' feature and teachers can see a 'History' of concerns. Students can also 'Report a concern' to a trusted teacher directly from their desktop – or the school's website out of school hours. In addition, its self-service directory of external online resources enables them to seek help outside of the school if they wish.

"All staff have a responsibility to provide a safe environment in which children can learn."

NetSupport School delivers a secure learning environment with its “Always-on” security settings, the ability to create lists of approved/restricted websites and control of portable media device use. NetSupport DNA offers a full safeguarding toolkit including tools such as alerting, monitoring, user profile creation, internet/application metering and USB endpoint security – to ensure systems are as safe, yet as flexible, as can be. There is now a ‘Health and Social Distancing’ AUP available to provide updates across the school - and a report to show who has read and accepted all AUPs.

“All staff should be prepared to identify children who may benefit from early help. Early help means providing support as soon as a problem emerges at any point in a child’s life, from the foundation years through to the teenage years.”

Having an insight into students’ activity is invaluable and could help facilitate an early intervention when students are engaged in activity that could place them at risk. NetSupport DNA provides teachers with this via its contextual intelligence-based Risk Index that produces a risk score for an individual student at that moment in time, meaning that teachers can intervene as necessary. They can also use the ‘Add a concern’ tool to make notes of a developing situation with a student. Vulnerable students can be marked as such within NetSupport DNA, enabling an extra layer of support.

“The designated safeguarding lead (and any deputies) are most likely to have a complete safeguarding picture and be the most appropriate person to advise on the response to safeguarding concerns.”

NetSupport DNA’s safeguarding module can be operated by safeguarding staff, independently of the IT team, ensuring confidentiality and enabling their professional response. When a safeguarding keyword is triggered, DSLs and supporting staff can now ‘tick’ or ‘untick’ it to highlight whether their review of the incident is complete; a useful feature to help staff track which ones need attention.

“All staff should be aware of systems within their school or college which support safeguarding and these should be explained to them as part of staff induction. This should include the child protection policy, behaviour policy, staff behaviour policy (sometimes called a code of conduct), safeguarding response to children who go missing from education; and the role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies). Copies of policies and a copy of part one of this document (KSCIE) should be provided to staff at induction.”

NetSupport DNA provides a flexible method of delivering and tracking policy distribution in a school; automatically presenting them to new staff to read, to all staff when updates have been applied, or to students to agree to an Acceptable Use Policy. The single upload saves time for administrators, who can assign the policy to a distribution list, and, as a bonus, ensures an accurate record is kept of who has seen and agreed to each policy. In response to the pandemic, a template is now also provided for a Health and Social Distancing AUP.

“All staff should be aware that safeguarding incidents and/or behaviours can be associated with factors outside the school or college and/or can occur between children outside of these environments. All staff, but especially the designated safeguarding lead (and deputies) should consider whether children are at risk of abuse or exploitation in situations outside their families. Extra-familial harms take a variety of different forms and children can be vulnerable to

multiple harms including (but not limited to) sexual exploitation, criminal exploitation, and serious youth violence."

Using sophisticated contextual AI risk analysis, NetSupport DNA extends the concept of context to factors within the school. The contextual intelligence-based Risk Index automatically assesses the context and history of a child's activities on the school's network – devices used, time of day, websites visited etc – and, from this, 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 in a lesson.

"All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting … put children in danger."

NetSupport DNA's Keyword and Phrase monitoring feature has a database of over 14,000 safeguarding terms, compiled with the Internet Watch Foundation and schools we work with – as well as including the Counter Terrorism Referral Unit (CTIRU) list (which schools can choose to enable or disable). When any terms in the database are triggered, staff can see these in a word cloud, enabling them to spot trending issues at a glance – and when reviewing these events, staff can highlight the status of their review by marking it as 'in progress' or 'complete', so all staff are aware.

"All concerns, discussions and decisions made, and the reasons for those decisions, should be recorded in writing..."

NetSupport School can provide a record of students' keyboard activity, website and application usage for that lesson, while in NetSupport DNA, using 'Report a concern', students can confide their worries to staff and attach screenshots, messages or other evidence to their concern record – and the teacher can add their own notes. Teachers can also 'Add a concern', if confided in verbally by a student. The 'History of concerns' tool means that safeguarding staff can track these over time – and the ability to re-assign them to another member of the safeguarding team means they are always visible.

"It is important for children to receive the right help at the right time to address risks and prevent issues escalating..."

Alongside all the alerting features in NetSupport DNA, teachers can also flag any students they know are particularly at risk as 'vulnerable' on the system – and even group these students together so they can be monitored in a single view. This makes it easier for concerned staff to keep an eye on these students, so they can act quickly if necessary.

"Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies, the ultimate lead responsibility to safeguarding and child protection ... remains with the designated safeguarding lead. This responsibility should not be delegated."

The structure of your safeguarding team can be defined in NetSupport DNA by setting up different safeguarding roles. The designated safeguarding lead who has overall responsibility can be assigned the 'Safeguarding Administrator' role that allows full access to all eSafety tools. The role of ‘Safeguarding User’ can then be applied to deputies and other members of the team for more streamlined access, if appropriate.

“Information sharing is vital in identifying and tackling all forms of abuse and neglect...”

For any serious safeguarding incident that needs to be referred to external agencies, evidence and records are key. The fact that NetSupport DNA records triggered keywords or reported concerns now forms an important part of an evidence trail – and that the school has been able to classify its vulnerable students demonstrates its vigilance. Any retrospective information required can be extracted from DNA either from its reporting tools – plus, depending on severity, triggered events are stored as a simple log, a screenshot or screen recording that provide the full background to an event.

“It is important that governing bodies and proprietors are aware that among other obligations, the Data Protection Act 2018 and the GDPR place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.”

NetSupport DNA’s GDPR toolkit can help school administrators to know exactly what data they hold by identifying all file types that may contain confidential information about students or staff. It also includes using tools to record whether the software used in the school is GDPR compliant in terms of the student personal data it stores. In addition, to help schools reduce the amount of sensitive data they keep, a data retention policy can be set to run and delete data of over a specified age.

“In addition, all staff should receive regular safeguarding and child protection updates ... to provide them with relevant skills and knowledge to safeguard children effectively.”

Any updated policies or information sheets can be distributed to staff via NetSupport DNA and senior leaders can see via its tracking who has read and acknowledged them. In addition, the opportunity for ad hoc safeguarding update training is provided as terms occur in the student-generated word cloud – meaning that staff can either share information between themselves or talk about topics with students, as necessary.

“As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.”

As students learn online digital citizenship skills, NetSupport School narrows the parameters of how far they can go with the ability for the teacher to create ‘allowed’ and ‘restricted’ website lists to ensure unsuitable sites are out of reach. NetSupport DNA also allows the creation of profiles to meet the need of each year group – ensuring that internet access is age appropriate, while allowing the students the flexibility to learn about the online world.

“Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that ‘over blocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.”

Over-blocking can mean that any potential safeguarding problems are simply shifted elsewhere, so NetSupport DNA offers teachers an insight into their students’ online activities so that they are aware of exactly what risks students are being exposed to, as well as being able to gauge their understanding of the elements of digital citizenship. Its flexible tools ensure that checks are in place to ensure a safe environment in which to learn.

"Since September 2019, Ofsted's inspections of early years, schools and post-16 provision are carried out under Ofsted's Education Framework. Inspectors will always report on whether or not arrangements for safeguarding children and learners are effective."

Both NetSupport DNA and NetSupport School retain all documentation electronically, making it easy to access and ensuring everything is covered. From tracking AUPs to monitoring any 'Report a concern' activity and outcomes (including archived reports and viewing the safeguarding keyword reports), staff can gain and demonstrate a greater understanding of safeguarding topics within their school. In addition, the GDPR toolkit helps schools ensure the protection of students' data, which ties into the confidentiality needed for safeguarding issues.

"Governing bodies and proprietors should ensure that their child protection policy includes: procedures to minimise the risk of peer on peer abuse ... [and] how allegations of peer on peer abuse will be recorded…"

NetSupport DNA's Keyword and Phrase monitoring can give teachers an insight into whether forms of peer on peer abuse are occurring, while at the same time helping to detect safeguarding issues across all topics – including any reference to upskirting (declared a criminal offence in April 2019). DNA's language packs also allow teachers to extend their safeguarding provision to a wider group of students, as the packs allow them to see and monitor phonetic representations of what students are typing in languages other than English.

"Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place."

In addition to web filtering with age-appropriate settings, NetSupport DNA's safeguarding toolkit allows schools to proactively and reactively safeguard students by alerting teachers to which students are engaged in concerning activity – and tracking application use for context to help avoid false alarms or over-blocking. Thanks to screen monitoring and alerts, safeguarding leads are alerted at the earliest opportunity and can take the appropriate action for each triggered event.

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, NetSupport Group
Date	30th June 2021
Signature	

Classroom .cloud

Company / Organisation	NetSupport Limited
Address	NetSupport House, Market Deeping, Peterborough, PE6 8NE
Contact details	01778 382270 / support@classroom.cloud
Monitoring System	**classroom.cloud** – cloud based Safeguarding & Classroom Management
Date of assessment	30th June 2021

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 classroom.cloud's Safeguarding keyword library.
- Utilisation of IWF URL list for the attempted access of known child abuse images	🟧	Not currently used.
- 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 but their URL blacklist Is not utlilised for filtering purposes in this solution.

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.
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.
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** 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.

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

Over-blocking can mean that any potential safeguarding problems are simply shifted elsewhere, so classroom.cloud offers schools an insight into their students' online activities so that they are aware of exactly what risks students are being exposed to, as well as being able to gauge their understanding of the elements of digital citizenship. Its flexible tools ensure that checks are in place to ensure a safe environment in which to learn.

classroom.cloud allows the level of enforcement by the product to be tailored to meet individual needs and can be set to exclude selected applications/websites, adapt monitoring 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.

As well as the Safeguarding component, classroom.cloud also offers a dedicated Teacher Console, utilising NetSupport's 30 plus years expertise in delivering market leading Classroom Management tools. This provides the flexibility for individual teachers to apply restrictions relevant to the current lesson.

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	🟨	Age-appropriate grouping (coming soon): You can create groups of student devices and apply specific settings to them. So, for example, students in year/grade 9 or identified as vulnerable, may have different online safety settings to those who are in year/grade 11.

• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	Safeguarding alerts are managed solely by the school. Custom 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. Safeguarding users also have the intuitive real time product dashboard at their disposal. 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.
• 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 school is in full control of which devices are monitored and determines, via the products Privacy Settings, the times when monitoring is live. Before any device can be monitored, the school will need to deploy the classroom.cloud Student (Remote Agent) application to it. Keyword Monitoring is currently supported on Windows and Chrome OS.
● 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	🟩	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.)

	🟩	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. If an account is terminated by NetSupport then all data will be removed immediately. While the subscription continues to be live, historical data will be retained for a rolling 13-month period, data older than 13 months will be purged from the system. Information relating to triggered keywords, as outlined earlier, is retained.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	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.

	🟩	
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	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. 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.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	classroom.cloud is designed for use in multi or single site environments. 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. The global Admin can then appoint individual ‘Site’ 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. Therefore, with this hierarchal approach, safeguarding alerts can be viewed and managed locally or organisation wide.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	Schools are encouraged to have acceptable use policies in place for monitoring. Within classroom.cloud, at a global or local level, phrase monitoring can be enabled or disabled with a single click. Similarly, privacy settings, applied across the organisation or locally, determine when monitoring is in force. 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.
• 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 are prioritised from Low to Urgent. 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. Keywords in the Suicide and Self-Harm libraries are flagged as High priority by default to ensure they are immediately visible. 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 therefore quickly identify vulnerable students with ease. 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. 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.
• 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.	🟩	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. However, potential privacy issues with this model are respected. 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. Settings can be applied by time of day (school hours), date (term dates), and you can restrict monitoring to just school network addresses/WiFi.
• Reporting – how alerts are recorded within the system?	🟩	The system offers a wealth of on-screen reporting options and

	🟩	views to allow Safeguarding Users to review alerts quickly and efficiently. As described previously, the dashboard is highly configurable, allowing you to filter views by category, priority, risk, device/user and more. The ability to quickly switch from the Phrase Cloud to a graphical representation or a detailed list, ensure maximum flexibility when reviewing the alerts. 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.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)	🟩	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.

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

classroom.cloud delivers a powerful combination of classroom management features for in-school and remote teaching and learning, along with the necessary Safeguarding tools to keep children safe as they learn.

This two-pronged approach helps schools meet their safeguarding requirements in line with the KCSIE guidance as follows. (The relevant extracts of the guidance are provided for context):

"**School and college staff are particularly important as they are in a position to identify concerns early, provide help for children, and prevent concerns from escalating.**"
With the help of its Keyword and Phrase monitoring tool and via Monitor Mode in the Teacher Console, teachers can gain an insight into students' activity as they use school technology.

"All staff have a responsibility to provide a safe environment in which children can learn."
classroom.cloud help schools deliver a secure learning environment with its configurable security and privacy settings and the ability to create lists of approved/restricted websites.

"All staff should be prepared to identify children who may benefit from early help. Early help means providing support as soon as a problem emerges at any point in a child's life, from the foundation years through to the teenage years."
Having an insight into students' activity is invaluable and could help facilitate an early intervention when students are engaged in activity that could place them at risk. classroom.cloud provides safeguarding leads with this via its contextual intelligence-based Risk Index that produces a risk score for an individual student at that moment in time, meaning staff can intervene as necessary.

"The designated safeguarding lead (and any deputies) are most likely to have a complete safeguarding picture and be the most appropriate person to advise on the response to safeguarding concerns."
classroom.cloud's safeguarding module can be configured to ensure that only designated safeguarding staff can operate it, independent of the IT team and teachers. (Although you can assign multiple roles to a user if, for example, teaching duties are combined with a Safeguarding role). When a safeguarding keyword is triggered, DSLs and supporting staff can highlight whether their review of the incident is in progress or complete and add progress notes.

"All staff should be aware that safeguarding incidents and/or behaviours can be associated with factors outside the school or college and/or can occur between children outside of these environments. All staff, but especially the designated safeguarding lead (and deputies) should consider whether children are at risk of abuse or exploitation in situations outside their families. Extra-familial harms take a variety of different forms and children can be vulnerable to multiple harms including (but not limited to) sexual exploitation, criminal exploitation, and serious youth violence."
Using sophisticated contextual AI risk analysis, classroom.cloud extends the concept of context to factors within the school. The Risk Index automatically assesses the context and history of a child's activities on the school's network – devices used, time of day, websites visited etc – and, from this, 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 lesson time 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 and associated with a lesson.

"All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting … put children in danger."

classroom.cloud's keyword and phrase monitoring feature has a database of over 14,000 safeguarding terms and covers many of the most commonly spoken dialects in UK schools. Our own research combined with our work with the Internet Watch Foundation, leading charities and local schools ensure trending topics are catered for across the spectrum of bullying, mental health, drug and alcohol abuse, gambling, sexual and criminal exploitation, racism, homophobia, radicalisation and more. When any terms in the database are triggered, staff can see these in a word cloud, enabling them to spot trending issues at a glance or can drill down into an individual student's triggers – and when reviewing these events, staff can highlight the status of their review along with accompanying notes so colleagues are aware.

"All concerns, discussions and decisions made, and the reasons for those decisions, should be recorded in writing..."
To supplement a schools own records and audit trails, classroom.cloud enables a detailed phrase match report to be printed or exported to file in order to help schools maintain a permanent log of activity.

"Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies, the ultimate lead responsibility to safeguarding and child protection ... remains with the designated safeguarding lead. This responsibility should not be delegated."
The structure of your safeguarding team can be defined in classroom.cloud by setting up different safeguarding roles. The designated safeguarding lead who has overall responsibility can be assigned the 'Safeguarding Administrator' role that allows full access to all safeguarding tools. The role of 'Safeguarding User' can then be applied to deputies and other members of the team for more streamlined access, if appropriate.

"Information sharing is vital in identifying and tackling all forms of abuse and neglect..."
For any serious safeguarding incident that needs to be referred to external agencies, evidence and records are key. The fact that classroom.cloud records triggered keywords forms an important part of an evidence trail – and that the school has been able to classify its vulnerable students demonstrates its vigilance. Any retrospective information required can be extracted from classroom.cloud's reporting tools – plus, depending on severity, triggered events are stored as a simple log, a screenshot or screen recording that provide the full background to an event.

"As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material."
As students learn online digital citizenship skills, classroom.cloud narrows the parameters of how far they can go with the ability for the teacher to create 'allowed' and 'restricted' website lists to ensure unsuitable sites are out of reach. At an administrative level, 'friendly' website lists can be created and set to be either monitored or not monitored.

"Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding."
Over-blocking can mean that any potential safeguarding problems are simply shifted elsewhere, so classroom.cloud offers teachers an insight into their students' online activities so that they are aware of exactly what risks students are being exposed to, as well as being able to gauge their understanding of the elements of digital citizenship. Its flexible tools ensure that checks are in place to ensure a safe environment in which to learn.

“Governing bodies and proprietors should ensure that their child protection policy includes: procedures to minimise the risk of peer on peer abuse ... [and] how allegations of peer on peer abuse will be recorded…”
classroom.cloud’s keyword and phrase monitoring can give teachers an insight into whether forms of peer on peer abuse (send nudes etc) are occurring, while at the same time helping to detect safeguarding issues across all topics – including any reference to upskirting (declared a criminal offence in April 2019). Language packs also allow teachers to extend their safeguarding provision to a wider group of students, as the packs allow them to see and monitor phonetic representations of what students are typing in languages other than English.

“Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to … risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.”
In addition to web management, classroom.cloud’s safeguarding toolkit allows schools to proactively and reactively safeguard students by alerting teachers to which students are engaged in concerning activity – and tracking application use for context to help avoid false alarms or over-blocking. Thanks to screen monitoring and alerts, safeguarding leads are alerted at the earliest opportunity and can take the appropriate action for each triggered event.

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, NetSupport Group
Date	30th June 2021
Signature	