Appropriate Monitoring for Schools

May 2025

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 by NetSupport – IT Asset Management and safeguarding
Date of assessment	1 October 2025

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 utilised.
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		NetSupport has worked with the CTIRU since Autumn 2016 and the police-assessed list of unlawful terrorist content (URL blacklist) is integrated into our NetSupport DNA 'on-prem' monitoring software.
• Confirm that monitoring for illegal content cannot be disabled by anyone (including any system administrator) at the school		To give our customers maximum flexibility in how they use our software, we do give schools the option to disable monitoring in NetSupport DNA if required, but the main system admin can avoid inadvertent enabling/disabling of the software by colleagues by applying appropriate permissions to each portal user role.

Illegal Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following illegal content

Content	Explanatory notes – Content that:	Rating	Explanation
child sexual abuse	Content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties.		We have integrated grooming/child abuse (IWF keywords) keyword libraries in our monitoring software. This means we can monitor all content typed, copied or seen within any application that would suggest a young person is vulnerable to exploitation in these areas. 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.
controlling or coercive behaviour	Online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts.		Integrated grooming/child abuse (IWF keywords) keyword libraries in our monitoring software. This means we can monitor all content typed, copied or seen within any application that would suggest a young person is vulnerable to exploitation in these areas. 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.
extreme sexual violence	Content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law.		Integrated safeguarding keyword libraries in our monitoring software mean we can detect text typed, copied or seen within any application that would indicate exposure to or promotion of extreme sexual violence. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.
extreme pornography	Pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful.		NetSupport DNA's safeguarding keyword libraries include terminology associated with extreme or obscene sexual material. The system monitors all text typed, copied or seen within applications or browsers, identifying when users may be exposed to, or attempting to access, such content. Phrase matches are graded by contextual risk level within the safeguarding console, allowing designated staff to intervene appropriately. Integration with the CTIRU list also prevents access to known illegal or high-risk domains. NetSupport DNA

			does not include image analysis or visual content detection.
fraud	Deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities.		NetSupport DNA's safeguarding keyword libraries include terminology associated with scams, fraud and phishing activity, helping schools identify attempts to engage in or access deceptive online content. The system monitors all text typed, copied or seen within applications or browsers and logs alerts within the safeguarding console, graded by contextual risk. Internet metering further supports visibility of potential exposure to fraudulent websites. While NetSupport DNA provides awareness of fraud-related behaviour, it does not perform real-time phishing or transaction detection.
racially or religiously aggravated public order offences	Content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion.		NetSupport DNA's safeguarding keyword libraries include terminology associated with racism, religious hatred and extremist language. The system monitors all text typed, copied or seen within applications or browsers that promotes or incites hatred or violence based on race or religion. Alerts are logged and graded by contextual risk level within the safeguarding console to support timely intervention. Integration with the CTIRU list also ensures access to known hate or extremist websites is blocked and logged.
inciting violence	Online material that encourages or glorifies acts of violence, posing significant risks to public safety and order.		NetSupport DNA's safeguarding keyword libraries include terminology linked to violence, aggression, extremism and the glorification of violent acts. The system monitors all text typed, copied or seen within applications or browsers that promotes or encourages violent behaviour. Phrase matches are graded by level of risk using the contextual intelligence-based risk

			indexing tool and logged within the safeguarding console for review by designated staff. Integration with the Counter Terrorism Internet Referral Unit (CTIRU) list also prevents access to websites known to promote or incite violence, ensuring comprehensive coverage.
illegal immigration and people smuggling	Content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation.		There is no dedicated keyword category for illegal immigration or people smuggling. However, NetSupport DNA's safeguarding libraries, including those covering grooming, sexual exploitation, criminal activity and radicalisation, contain terminology linked to trafficking and exploitation. The system monitors all text typed, copied or seen within any application or browser, with phrase matches graded by level of risk using the contextual intelligence-based risk indexing tool. Alerts are logged within the safeguarding console to support timely intervention and appropriate follow-up by designated staff.
promoting or facilitating suicide	Material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations.		Separate suicide and wellbeing keyword libraries monitor all text typed, copied or seen within any application that indicates a young person is considering suicide or being exposed to material encouraging or facilitating suicide. Our ongoing research and work with specialist partners and charitable organisations ensure these libraries remain current. Keywords in this category are automatically assigned high-priority status to raise the profile of alerts to safeguarding staff.
intimate image abuse	The non-consensual sharing of private sexual images or videos, commonly known as "revenge porn," intended to cause distress or harm.		NetSupport DNA's safeguarding keyword libraries include terminology linked to sexual exploitation, grooming, coercion and blackmail, which can indicate risks associated with the sharing

			of intimate images. The system monitors text typed, copied or seen within any application or browser and grades phrase matches by level of risk using the contextual intelligence-based risk indexing tool. While DNA detects textual indicators of image-based abuse, it does not perform image analysis or visual content detection.
selling illegal drugs or weapons	Online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations.		Drugs and weapons keyword libraries in NetSupport DNA detect text typed, copied or seen within any application that relates to the sale, purchase or promotion of illegal substances or weapons. Slang and alternative terminology are included to capture emerging trends, ensuring comprehensive detection. Phrase matches are graded by contextual risk level within the safeguarding console to support appropriate follow-up.
sexual exploitation	Content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution.		Integrated grooming and sexual exploitation keyword libraries in our monitoring software detect text typed, copied or seen within any application that indicates coercion, manipulation or exploitation for sexual purposes. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool. Alerts are logged within the safeguarding console for review and intervention by designated safeguarding staff.
Terrorism	Material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.		The radicalisation keyword library in our monitoring software detects text typed, copied or seen within any application that indicates exposure to, or promotion of, terrorist or extremist material. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool, supporting schools to identify potential concerns and

			enable timely safeguarding intervention.

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
Gambling	Enables gambling		The gambling keyword library in our monitoring software detects text typed, copied or seen within any application that relates to gambling, betting or online gaming for financial gain. It includes terminology linked to addiction and betting apps to help identify vulnerable users. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.
Harmful content	Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.		NetSupport DNA includes safeguarding keyword libraries designed to identify harmful content, including language linked to bullying, harassment, hate speech, violent or abusive behaviour, and the encouragement of dangerous behaviour. The system monitors text typed, copied or seen across supported applications and browsers, helping schools identify potential risks to wellbeing. Phrase matches are logged within the Online Safety portal and graded by contextual risk level using the system's intelligence-based risk indexing tool, ensuring staff can prioritise concerns appropriately.
Hate speech / Discrimination	Content that expresses hate or encourages violence towards a person or group based on something such as race, religion, sex, or sexual orientation. . Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010		Integrated safeguarding keyword libraries in our monitoring software include terms linked to hate speech, discrimination and intolerance. The system monitors all text typed, copied or seen within any application that expresses or promotes prejudice, hostility or violence towards

			protected groups. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content, including ransomware and viruses		NetSupport DNA supports schools in identifying activity linked to system compromise, hacking or filter-bypass attempts through its safeguarding keyword libraries and internet metering tools. The system monitors for terminology related to hacking, VPNs, and proxy use, and records attempts to access associated sites or tools. Integration with the Counter Terrorism Internet Referral Unit (CTIRU) list enables automatic blocking and logging of access to known malicious or high-risk domains. While DNA does not scan for malware or viruses, it provides visibility of behaviour that could indicate exposure to such threats, supporting schools in maintaining a secure and policy-compliant environment.
Mis / Dis Information	Promotes or spreads false or misleading information intended to deceive, manipulate, or harm, including content undermining trust in factual information or institutions		NetSupport DNA does not analyse or fact-check online content for accuracy. It cannot determine whether information viewed or shared is true or misleading. However, its safeguarding keyword libraries include terms linked to extremism, conspiracy theories and online manipulation, helping to identify when users may be exposed to or engaging with harmful narratives. These keyword triggers are logged within the eSafety console and graded by contextual risk level to support appropriate intervention.
Pornography	displays sexual acts or explicit images		NetSupport DNA detects text and search activity associated with pornographic or sexually explicit material through its safeguarding keyword libraries and internet metering tools. Attempts to

			access related websites or searches are recorded and graded by contextual risk level within the Online Safety console. Schools can also block and log access to such sites through custom URL restrictions. NetSupport DNA does not perform image analysis or detect explicit visual content.
Self Harm and eating disorders	encourages, promotes, or provides instructions for self harm or eating disorders		Separate self-harm and eating disorders keyword libraries in our monitoring software detect text typed, copied or seen within any application that indicates vulnerability, distress or engagement with self-harm or disordered eating behaviours. Our ongoing research and collaboration with specialist partners ensure these libraries remain current. Keywords in this category are automatically assigned high priority status to raise the profile of alerts to safeguarding staff.
VAWG	Promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.		Integrated safeguarding keyword libraries in our monitoring software include terms linked to violence, coercion, misogyny and harmful gender stereotypes. The system monitors all text typed, copied or seen within any application that promotes or normalises gender-based violence or abuse. Phrase matches are graded by level of risk using our contextual intelligence-based risk indexing tool.

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

NetSupport DNA's safeguarding technology is designed to help schools meet their statutory safeguarding duties by monitoring content typed, copied or seen within applications, browsers and online communication platforms. The system's keyword libraries, developed in collaboration with safeguarding specialists and community partners, are continually updated to reflect emerging risks, trends and slang across multiple languages. Schools can add their own custom terms to reflect local safeguarding priorities and opt to share them with NetSupport for wider inclusion in future updates.

Keyword alerts are graded by level of risk using the contextual intelligence-based risk indexing tool, ensuring that safeguarding teams can quickly identify and support vulnerable students.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age 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		With NetSupport DNA, schools can create online safety groups and apply tailored safeguarding settings to each. This allows staff to configure which keyword categories are active, determine who receives alerts, and manage student visibility within the 'Report a concern' tool. These group-based settings ensure monitoring remains appropriate to the age and needs of different cohorts while supporting proportionate safeguarding oversight.
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		Safeguarding administrators can configure which priority levels and keyword categories trigger alerts for each user role. Alerts rated Medium and above generate email notifications to nominated safeguarding staff. In the online safety portal, new alerts are flagged as "new" until reviewed; they can be annotated, forwarded, reassigned or dismissed. For schools using CPOMS or Tes MyConcern, triggered events and reported student concerns can be linked directly to the corresponding student in those systems via integration. Existing alert configurations can be adjusted or removed at any

		time through the admin interface.
• 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.		An Audit Log records actions, system changes and configuration updates made by all NetSupport DNA users across each site. Events such as adding/removing users or devices, licence changes and deleting false-positive triggers are all captured. These audit entries cannot be disabled or removed and may be filtered, searched or exported to support accountability and oversight.
• BYOD (Bring Your Own Device) – if adopted by the school and 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		NetSupport DNA does not directly monitor personal BYOD devices. Its safeguarding and IT asset management features apply only to school-managed devices enrolled within the DNA environment. When students or staff use personal devices, DNA can monitor network activity that passes through the school infrastructure, such as when devices connect to the school network or Wi-Fi, allowing alerts related to browsing or network use to be logged centrally. Schools adopting a BYOD model should ensure that their BYOD or Acceptable Use Policy clearly outlines how personal devices connect to the network and how data is managed. NetSupport DNA operates entirely within school hours and locations defined by the network parameters and does not collect or monitor data from personal devices outside these boundaries, ensuring compliance with GDPR and safeguarding best practice.

• 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		NetSupport DNA is an on-premises solution, meaning all data is stored locally on the school's or trust's own infrastructure and remains under their direct control. No safeguarding, user or system data is transmitted to or stored in the cloud. The system database, hosted within the school's secure network, stores configuration data, device inventories, user activity logs, and safeguarding records for as long as determined by the school's retention policy. Schools can define their own data-retention periods and apply scheduled data-purge options within the DNA console to automatically remove historical records after a defined time frame. Data backups are the responsibility of the school's IT team and should follow the school or trust's existing data-protection and disaster-recovery procedures. All access to stored data is governed by administrator permissions within DNA, ensuring that only authorised users can view or export information.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		NetSupport DNA requires the installation of a lightweight client agent on each managed device to enable monitoring, safeguarding and asset management functionality. The DNA Agent supports from Windows 7 onwards. and Server 2008 R2 or later, DNA Server - SQL Server 2008 or later. If no version of SQL exists on the target system when installing the

		DNA Server, users will be prompted to either install SQL (SQL Server 2019 Express is included in the NetSupport DNA setup file. This is only supported on Windows 10, Windows Server 2016 and above) or to specify the address of an existing SQL Server. macOS (Catalina 10.15 or later) is also supported. For Chromebooks, a dedicated Chrome Agent provides internet and safeguarding keyword monitoring when using the Chrome browser. On iOS and Android devices, the NetSupport DNA browser app allows keyword monitoring, internet activity tracking and access to the "Report a concern" feature - providing safeguarding visibility in line with mobile operating system restrictions. All data collected by the agents remains within the school's secure, locally hosted DNA server. Deployment of agents can be managed manually or centrally using tools such as Active Directory Group Policy, Microsoft Intune or MSI packages. The software requires a 64-bit operating system and administrator permissions for initial setup. NetSupport DNA console supports Windows 7 or higher.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended according to an agreed policy		Schools can amend safeguarding keyword coverage in line with policy. Administrators can add custom keywords, adjust the priority of existing phrases, and enable or disable

		keyword libraries for specific groups or at site level. Changes take effect immediately and are recorded in the audit log for accountability. This ensures schools can respond quickly to emerging vocabulary or local risks across all supported languages.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		NetSupport DNA provides robust multi-site management capabilities, allowing multi academy trusts, federations and local authorities to centrally deploy, monitor and manage settings across all connected schools or sites. The hierarchical structure enables central administrators to define organisational policies, configure keyword libraries and manage safeguarding alerts at group level while delegating local permissions and visibility to school-based safeguarding leads. Data from each site is securely transmitted to the organisation's DNA server, supporting centralised reporting, alert escalation and oversight via the console dashboard. Administrators can configure site-specific or global settings, ensuring consistency with local flexibility. This structure allows safeguarding and IT leads to monitor all alerts, keyword triggers and trends from a unified management console while retaining site-level autonomy for context-sensitive decisions.
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (e.g. Image hash).		NetSupport DNA does not include image analysis or visual content scanning. Its

		safeguarding capabilities focus on text-based monitoring, capturing words and phrases typed, copied, or seen within supported applications and browsers. The system detects safeguarding concerns through contextual keyword analysis across multiple categories, including adult content, drugs, racism, radicalisation, and weapons. While DNA does not analyse or hash visual content, alerts triggered by contextual keywords can still identify behaviour suggesting potential exposure to harmful imagery, allowing designated safeguarding leads to investigate promptly.
• Identification - the monitoring system should identify users and devices to attribute activity (particularly for mobile devices) and ensure the application of appropriate configurations for individual users.		NetSupport DNA attributes safeguarding and activity data to identified users and devices through its integration with Active Directory. Each event or trigger is automatically linked to the logged-in Windows user account, device name, time, and location, ensuring full traceability. DNA also records the device's hostname and IP address, allowing administrators to verify activity at both individual and site levels. While NetSupport DNA primarily operates on network-connected Windows and macOS devices, its identification is dependent on the user being logged into a domain-joined system; mobile device attribution is not supported outside this environment.

• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		NetSupport DNA provides schools with full control over their monitoring policies and visibility of user notifications. When the DNA Agent is installed on a user's device, the system displays a configurable notification icon in the system tray, making users aware that monitoring is active. Schools can customise this message within their Acceptable Use and Privacy Policies to ensure transparency. NetSupport provides supporting materials, including Privacy by Design documentation, a Data Processing Agreement, and guidance for inclusion in school policies and parental communications. This helps schools explain the safeguarding and network-management purpose of monitoring clearly to students, staff and parents, aligning with UK GDPR and KCSIE expectations.
• Mobile and app content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the monitoring system operate across mobile devices and app content. Providers should be clear about the capability of their monitoring system to monitor content on mobile and web apps and any configuration or component requirements to achieve this.		NetSupport DNA supports safeguarding on Chrome OS via a dedicated Chrome Agent extension, enabling keyword monitoring, internet metering and "Report a concern" functionality within the browser. Schools may centralise deployment via Google Admin. On Windows and macOS devices, full client agents monitor text typed, copied or seen across applications and browsers. NetSupport DNA does not currently support app-level monitoring outside the browser on mobile operating systems (iOS, Android).

• Multiple language support – the ability for the system to manage relevant languages?		NetSupport DNA includes safeguarding keyword libraries in multiple languages, including English, French, German, Spanish and Italian. Schools can add their own custom keywords in any language, which can then be prioritised or shared with NetSupport for future inclusion. All keyword activity is processed through the contextual intelligence-based risk indexing system to ensure consistency in alert grading. The DNA console and reporting tools also support multiple display languages for staff access.
• 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?		NetSupport DNA uses a contextual intelligence-based risk index to prioritise safeguarding events. Each keyword trigger is automatically assessed for severity, context and frequency, and then assigned a risk level (Low, Medium, High, Critical). High and Critical events generate alerts for designated safeguarding users via the NetSupport DNA console and, where configured, by email. The system records user, device, time and application details to support rapid investigation. Safeguarding leads can review, acknowledge or escalate alerts directly within the console, ensuring timely intervention and accountability.
• 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. Monitoring should focus on school-owned and managed devices. When		NetSupport DNA supports remote safeguarding for school-owned devices through the DNA Gateway, enabling keyword and activity monitoring when devices are used off-site. All

shared devices are used, schools must ensure users log in individually. This allows monitoring systems to apply restrictions and configurations based on user profiles, improving the safeguarding process.		safeguarding alerts, logs and contextual risk analysis remain visible in the NetSupport DNA console, ensuring continuity of oversight. The Gateway configuration allows schools to manage how and when remote monitoring is active, ensuring compliance with local safeguarding and data protection policies.
• Reporting – how alerts are recorded within the system?		Safeguarding alerts in NetSupport DNA are recorded within the Safeguarding console, capturing the student, device, site, application, time and contextual details. Alerts are automatically prioritised using the contextual risk index and can be filtered, searched or exported by category, user or date to identify patterns or emerging risks. NetSupport DNA integrates directly with CPOMS and Tes MyConcern, ensuring accurate transfer of safeguarding information. All reporting actions are captured within the audit log and alert histories remain available in line with school data retention settings.
• Safeguarding case management integration – the ability to integrate with school safeguarding and wellbeing systems to better understand context of activity		NetSupport DNA has an export feature so that you can upload records from DNA into CPOMS or Tes MyConcern. There isn't currently a direct API link that connects NetSupport DNA to a school safeguarding solution.

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 does not provide a third-party proactive monitoring service or external moderation team. All safeguarding alerts are managed internally by the school's designated safeguarding leads through the NetSupport DNA console; this is because there is no one better

placed to understand a setting's context than the setting itself. The system applies automated contextual analysis and risk weighting to categorise alerts by priority, helping staff focus on those requiring immediate attention. Schools are supported through built-in guidance and training materials to strengthen their own safeguarding capability and ensure consistent, informed responses to triggered events.

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

NetSupport DNA actively supports schools in meeting their statutory safeguarding duties under the latest *Keeping Children Safe in Education (KCSIE)* guidance. The platform provides comprehensive keyword and phrase monitoring, user activity tracking and safeguarding alerts aligned with KCSIE expectations for appropriate filtering and monitoring. These are supported by extensive reporting, audit trails and data protection controls.
As part of the broader NetSupport suite, DNA includes built-in safeguarding features such as keyword libraries developed in consultation with schools and child protection professionals, a "Report a concern" feature for pupils, and detailed oversight tools for safeguarding leads.
NetSupport provides training, webinars and guidance materials, including sessions led by CEO Al Kingsley MBE and Mark Anderson, to help schools interpret updates to statutory guidance, evidence compliance and strengthen their safeguarding culture.
Together, these tools and resources help ensure schools can demonstrate compliance, transparency and best practice in line with KCSIE and wider DfE expectations.

How does your monitoring system identify and respond to activity involving Generative AI technologies (e.g. AI prompts, content creation, or platform use)?
In your response, please explain how your system captures or analyses user interactions with Generative AI tools; to what extent logs or alerts reflect potential safeguarding risks associated with AI-generated content (such as harmful prompts or inappropriate use of image and text generation); any known limitations—whether technical, privacy-related, or device-specific—that may affect your system's ability to monitor such activity; and what guidance you provide to schools to support their understanding and management of Generative AI-related risks.

NetSupport DNA supports schools in monitoring the use of generative AI platforms by analysing text typed, copied or seen across supported applications on managed devices. This allows schools to identify interactions with AI tools such as ChatGPT, Copilot or Gemini, and to detect inappropriate or harmful prompts that may raise safeguarding concerns. All detected phrases are logged within the Safeguarding Console and graded for contextual risk using NetSupport's built-in keyword weighting system, helping staff prioritise alerts effectively.
DNA does not analyse, interpret or assess the accuracy, bias or intent of AI-generated outputs, and it cannot access or review encrypted or off-network traffic. Monitoring applies only when devices are active and connected to the school network or DNA Agent, ensuring that data capture remains secure and proportionate.
To help schools manage emerging AI-related risks, NetSupport provides professional development and guidance through webinars, publications and training materials. These include the R.I.S.E. Magazine "Getting Started" series, ListEd podcast, and recent sessions hosted by NetSupport's CEO, Al Kingsley MBE, and Mark Anderson (Head of Education) focused on responsible AI use, online safety, and KCSIE compliance.
Together, these tools and resources equip schools to interpret AI-related activity confidently, support digital literacy and maintain a proactive safeguarding approach aligned with DfE and UKSIC standards.

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	Al Kingsley
Position	CEO
Date	25th November 2025
Signature