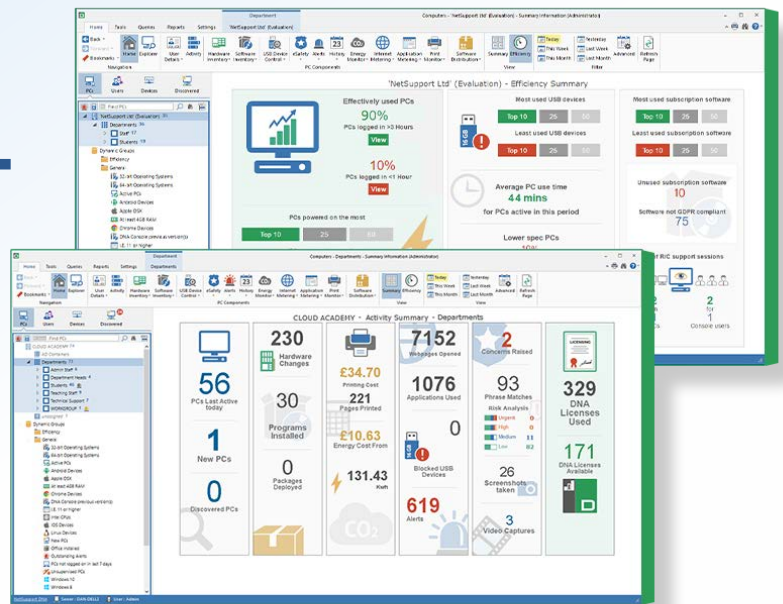# NetSupport DNA

Network and IT Management
for school or campus networks

The complete solution for managing school technology

NetSupport DNA is an award-winning, easy-to-use solution that provides schools with the tools to manage technology in the classroom, as well as across the school and campus, while safeguarding students and supporting teachers.

Armed with a complete overview of school IT activity, NetSupport DNA helps technicians work smarter whilst maintaining a secure and reliable network. From staying ahead of any potential IT issues before they escalate, to automating tasks, NetSupport DNA not only helps save time but also boosts security and productivity.

It gathers a wealth of device and usage data (up to 10,000 devices) to inform decision making and allow accurate planning of future IT spending and refresh plans.

What's new?

IT technicians across a school now have a more flexible and efficient way to carry out specific tasks on multiple staff/student devices. They can perform actions on multiple devices, such as messaging or running PowerShell commands – saving time and delivering extra convenience for technicians.

Internet risks and trends are constantly changing and, to keep students safe, NetSupport DNA's safeguarding/ online safety toolkit now has two new categories – Gambling and Cybersecurity – to help safeguarding staff see any related triggered events more quickly. Staff can also add notes to all triggered events (not just the false positives), such as details of any follow-up actions and more – perfect for ensuring other safeguarding staff are kept updated.

Key features:

- ✓ Hardware inventory and discovery
- ✓ Software licence management
- ✓ Internet metering
- ✓ Application metering
- ✓ Endpoint security and system-wide alerting
- ✓ Energy monitoring
- ✓ Power management
- ✓ Remote Control and admin tools
- ✓ User management
- ✓ Activity monitoring
- ✓ Multi-site support and management
- ✓ GDPR toolkit
- ✓ Safeguarding/online safety toolkit
- ✓ Classroom Management (optional)

Ease of installation

After installation of the server module (used to manage and add information to the DNA database), the deployment tool provided will automatically discover and install the DNA agent on targeted devices across the school (supports up to 10,000 devices). The DNA console (installed by the IT technician) provides full DNA system control, rich on-screen information and real-time reporting.

Hardware Inventory

NetSupport DNA provides one of the most comprehensive and detailed hardware inventory modules available. A wealth of information is gathered from each device – from CPU and BIOS types to network, video and storage information.

Inventory reports are displayed either for a single PC, a selected department, just teachers or a specific classroom PC, or condition-based "Dynamic Groups".

Hardware inventory updates are configured to run at different times throughout the day or at start-up and can be refreshed instantly on demand. A standalone inventory component is available to run on non-networked or mobile devices and, in addition, high value peripherals can also be associated and recorded against a device – perfect for keeping track of school assets.

Efficiency View

The unique dashboard highlights at a glance how school technology is being used and the areas where efficiency can be improved to create cost- and time-saving benefits, e.g. highlighting which PCs are least effectively used (and therefore can be redeployed) or which apps are the least used (and therefore may not need renewing).

SNMP device discovery

The SNMP Discovery view allows NetSupport DNA to be configured to scan a range of network addresses and report on any appropriate devices discovered across the school, such as printers and access points. These items can then be stored within DNA and real-time data (such as ink or toner levels) can be monitored from the console.

Energy Monitoring and Power Management

The Energy Monitoring module provides a concise high-level summary of potential energy wastage across computer systems left powered on out of school hours. It keeps an accurate record of when a computer is powered on, off or hibernates, to provide an average (and customisable) "power consumption per device" calculation. Now, you can set Power Management policies to automatically power computers off and back on at specific times – and "inactivity policies" for systems inactive over a period of time.

Internet Metering

The key to supporting an effective online safety policy is providing effective controls. With NetSupport DNA, internet usage can be fully managed: lists of approved and restricted URLs (including CTIRU list) and/or sub-URLs can be applied centrally to specific groups, allowing for age-appropriate group internet filtering. Once applied, NetSupport DNA can allow unrestricted access to all websites, restricted access to certain websites that have been marked as approved by the school or block access to specific sites marked as inappropriate. It also logs start and finish times for each URL visited and the active time spent on a page. Results can be reviewed by device or user. In addition to restricting websites and applications by their specific name, apps and games can be blocked or restricted by their window's title, helping technicians to add a broader layer of security while keeping students on task.

Software Inventory/Licensing

The Software module is designed to help schools better manage licence compliance and reduce software overspend by accurately reporting installed software and proactively identifying PCs with software that has no or low usage.

It supports the ongoing management of all software licences for each department: recording suppliers, purchase and invoice details, department or cost centre allocation and the tracking of maintenance contracts – as well as storing PDF copies of any supporting documents.

Software Application Metering

The Application Metering module reports on all applications used on each PC or server, detailing the time the application was started and finished, as well as the actual time it was active.

Monitoring application use ensures software licences are assigned to the right staff/students and aren't renewed without evidence of activity – thus enabling cost savings.

Application usage can also be restricted for students, either fully or just by time of day. Lists of approved and restricted applications, together with times when restrictions apply, can be created and enforced centrally.

Real-time monitoring

The Explorer mode provides a real-time overview of all PCs on the network, highlighting which ones have current notifications and active polices, to ensure operators can identify and resolve issues quickly. The data view can be presented as Icons, Details or Thumbnails (where the PC screens are visible). In Details mode, performance data such as real-time network traffic, CPU and memory use for each PC is displayed to give an instant view of network health. Privacy modes can be set to provide data protection

and confidentiality. Using Explorer mode, technicians can use the Spotlight feature to see more details about a selected PC (e.g. any applications, services, websites and processes in use), all in a single glance.

Software Distribution

NetSupport DNA provides a multi-delivery option for Software Distribution. A software distribution package is created by either applying parameters to a collection of files or folders or by using the DNA application packager – recording the user prompts, keystrokes and mouse clicks that are used during a test installation, and then automating these on a live deployment to bypass the need for operator intervention. NetSupport DNA also includes a Scheduling feature, allowing packages to be deployed on a specific date and time – usually out of core school hours when network traffic is at its lowest. An error report is also available to see whether there were any errors during the install.

School Alerting

DNA's powerful Alerting module automatically notifies operators when any number of changes occurs across the school network. The module is easy to use and there is no limit to the number of custom alerts that you can add.

System Error Alerts also capture screen shots/videos of system errors as they occur, for faster problem solving. This applies to all PC alerts, allowing you to choose what happens when any alert is triggered. You can direct alert notifications to specified email recipients and/or active console users (on a per alert basis, so the nature of the alert may dictate who is notified). In addition, outstanding alerts are identified against matching PCs on the main hierarchy tree view. Operators can add notes to alerts and a detailed log is accessible from the History feature.

Acceptable Use Policies

NetSupport DNA provides a flexible module to support the delivery and tracking of AUPs across the school. Policies can be applied to specific devices or users for display each time any user logs on or for one-time display and acknowledgement. The AUP feature can support multiple policies (including a new Health and Social Distancing policy), which can then be formatted for clear presentation. Full tracking and exception reporting are also provided.

Print Monitoring

Individual printers across the school are automatically identified and, from the central console view, costs for printing can be assigned either globally or against each printer. Where required, printers can also be excluded from the view. A full overview of printing activities and indicative costs is provided.

Vault

NetSupport DNA contains a Vault component to allow secure storage of serial numbers, passwords or any other confidential IT data. Access to the Vault can be restricted to specific console users and activity can be recorded against the central DNA audit trail.

Endpoint Security

To help maintain school network security, USB memory stick use can be controlled across the entire school or just specific departments, staff or students. You can choose settings to allow full access, block all access, allow read-only access or prevent applications being run from an unknown memory stick. Alternatively, you can authorise the use of individual memory sticks for the current day, a week or indefinitely – use can also be limited to only those authorised. It can also detect if USB drives are encrypted (Bitlocker).

User Management

NetSupport DNA provides a range of features to locate and manage users within a networked environment. Schools can customise the data to be gathered from each user, including the tracking of user acceptance forms. DNA also keeps a history of changes to User Data and records changes to custom user details. Profiles can be set for different groups of devices or users, each with its specific component settings, i.e. limited internet access for Year 7. NetSupport DNA can prevent or allow selected users to be logged on to multiple machines, allows users to locate another logged-on user and send them a message, plus enables teachers and technicians to reset students' system passwords. A single time-based summary of all activity by a specific user, PC or department (chronological view) is also available. Plus, technicians can remotely log in to multiple school PCs on the LAN, and also support remote schools that are not part of their main infrastructure via the secure inbuilt Gateway component. IT teams can also conduct a two-way chat session between any number of selected staff or students in full audio mode.

Safeguarding/online safety

NetSupport DNA's safeguarding/online safety toolkit contains a contextual intelligence-based Risk Index which automatically flags high-risk events and vulnerable students, based on sophisticated AI risk analysis.

The Keyword and Phrase Monitoring feature provides insight into and alerts from any activity by a student that might suggest they are engaged in activity that would place them at risk. The details/context of triggered words can be reviewed, with the results (available as a log, screenshot and screen recording, according to severity level). Triggered events can be marked as 'in progress' or 'complete' to let supporting staff know their status.

The "Report a concern" feature allows students to report concerns discreetly to nominated school staff. Teachers can also "Add a concern" where they are verbally told of a student's concern. Safeguarding staff can also flag at-risk students on the system so they can be easily identified and support provided to them.

System Audit
NetSupport DNA includes a powerful Audit component to track all selected console activity by staff. The Audit feature records changes to policies or settings – when entries are added/deleted, or where rights are changed for any user.

GDPR
NetSupport DNA contains a range of tools to help schools meet their GDPR requirements at no extra cost. The Software inventory helps you keep track of software installed and flag GDPR-compliant solutions. Using the Data Discovery tool, all or selected network PCs can quickly be scanned to identify pre-configured "GDPR relevant" file types that may contain staff or student data. In addition, schools can archive or remove all data history related to an individual stored within NetSupport DNA. With the remote control tools, technicians can also quickly access a PC or laptop on the network to remove or move any files that should not be there. To help schools reduce the amount of data they store, a Data Retention Policy can be scheduled to automatically delete data (such as internet/application metering,

login sessions, triggered online safety keywords and more) over 365 days old (default mode). The data can be backed up before the policy runs and emails can be sent to notify staff when the process is complete.

Reporting
NetSupport DNA provides both on-screen and print-optimised reporting. The on-screen reports/views are provided with supporting bar and pie charts and "live" drill down capabilities on all key summary data. As well as reporting on individual devices, users and departments, NetSupport DNA also features user-defined dynamic groups. A dynamic group could, for example, be to identify which classroom PCs are upgradeable and such a group would be created automatically from those that match the required criteria – such as "all PCs with more than 'XX' GB RAM" and so on.

Mobile Inventory
You can download NetSupport DNA's Mobile Console app free from the Google Play and Apple app stores. The app allows a technician, when away from their desk, to search for and view a detailed hardware/software inventory for any PC on campus. It also includes a QR code scanner to help instantly identify any PC: either from an on-screen QR code displayed by DNA, or from a label fixed to the device. NetSupport DNA also provides a QR code label creation facility that includes displaying custom details. The app also shows a history of all hardware changes, plus any software installs or removals.

We work with...

System Requirements

NetSupport DNA Server component
Minimum hardware: Single - Dual Core 2.00 GHz CPU, 8Gb RAM or higher. Free space required: 20 Gb. (dependent on number of Agents supported). Windows Server 2008 R2 or above (best practice). Windows 7, Windows 8.1, Windows 10, and Windows 11.
Databases supported: SQL Server 2008 or later. If no version of SQL exists on the target system when installing the DNA Server, you will be prompted to either install SQL (SQL 2019 Express is included in the NetSupport DNA setup file), or to specify the address of an existing SQL Server.

Optional Server modules (SNMP Discovery, Remote Gateways etc)
Windows 7 or higher. Windows Server 2008 SP2 or higher.

NetSupport DNA Management Console
Free space required: 200 MB
Windows 7 or higher. Windows Server 2008 R2 or higher.

DNA Mobile Console apps
Android 5 or higher. iOS 9.3 or higher.

DNA Desktop Agent (client)
Free space required: 25 MB
Windows Vista or higher.
Windows Server 2008 or higher.
macOS 10.8 or higher.
Chrome (agent available).

NetSupport iOS Browser app
iOS 9.3 or higher. (Requires V4.8 of DNA console)

NetSupport Android Browser app
Android 5.1 or higher. (Requires V4.8 of DNA console)