NETSUPPORT DNA, DATA PROTECTION, PRIVACY AND COMPLIANCE

Introduction

As a publisher of software designed to help organisations deliver learning outcomes, we recognise that there is an onus on us to help those organisations understand how to use the functionality and ensure the safety and security of any personal information involved. This is no different with NetSupport DNA, our award-winning IT Asset Management and Safeguarding tool.

This document is aimed at UK/EU customers but also supports best practices and advice for other regions (e.g., US – COPPA/FERPA). Ultimately, we hope it provides you with a better understanding of where we can help you and your subsequent responsibilities.

UK/EU GDPR

The **EU General Data Protection Regulation ("GDPR")** came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the EU GDPR has been designed to meet the requirements of the digital age. Subsequently, upon leaving the EU, the **Data Protection Act 2018** was updated to enact the **UK GDPR**, replicating the EU GDPR.

The UK GDPR aims to standardise the regulation of data protection laws and processing across the UK and work alongside the EU regulations, as well as influence other legislation across the globe – affording individuals stronger, more consistent rights to access and control of their personal information.

NetSupport DNA is a suite of easy-to-use tools for managing and supporting IT assets across a schoolnetwork or campus. Its features include automatic discovery of devices; hardware and software inventory; change tracking and software licence management; energy monitoring; power management; USB endpoint security; printer monitoring; application and internet metering; a flexible alerting suite; and an easy-to-use software distribution module. NetSupport DNA also supports eSafety and safeguarding with keyword and phrase monitoring to alert schools of any online activity that may place a student at risk; internet monitoring of websites visited; the option for students to report concerns directly to trusted staff; and more.

A NetSupport DNA installation processes personal data and, as such, is impacted by the GDPR. This document will provide you with all the information you need relating to NetSupport DNA to ensure that personal data is processed in accordance with the GDPR and other relevant data protection and privacy legislations. The following sections are designed to help you with your Record of Processing Activities, any risk assessments you may need to complete, any due diligence needed during purchase/procurement and to help you with information you may need for your Privacy Notice.

COPPA and FERPA compliance (USA)

Children's Online Privacy Protection Act of 1998 (COPPA) places requirements on operators of websites or online services directed to children under the age of 13 years old, and on operators of websites or online services that have actual knowledge that they are collecting personal information online from a child under the age of 13 years. The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. It protects personally identifiable information (PII) in students' information records from unauthorised disclosure.

NetSupport DNA fully meets the requirements for compliance as it is a fully on-premise solution. No data is shared with NetSupport or third-party services, and any information collected within NetSupport DNA is solely used for the purpose of the management of devices, software and users, any activities on the devices (including where safeguarding triggers occur) and associated operational functions as part of support and management of IT infrastructure and Governance (remote control, AUP, etc.).the continued classes.

How does NetSupport DNA process personal data?

NetSupport DNA uses an agent installed on computers to gather inventory, usage and safeguarding data. The NetSupport DNA Agent will record the following information:

HARDWARE INVENTORY

The details of which hardware inventory details are recorded are generally irrelevant to GDPR as these are not considered personal data and therefore will not be listed in this document. Exceptions to this will include where hardware information can be combined with other information to create personal data (e.g. IP address, device names, groups, etc.)

SOFTWARE INVENTORY

As with hardware inventory, the software inventory is not classed as personal data and is therefore not detailed in this document.

USAGE INFORMATION

The following usage information may be recorded:

- All log on, log off, lock and unlock events
- All power on, power off events
- All applications started and closed
- All websites visited
- All print jobs set to printers.

SAFEGUARDING INFORMATION:

When the DNA agent matches one of the configured safeguarding phrases, the following information may be recorded:

- The phrase that was matched and the context it was used in (if the work was typed).
- A picture taken from the webcam, if present.
- A screenshot of the screen at the time the phrase was matched.
- A video showing the computer screen before and after the phase was matched.
- If the device has a webcam, then this can be configured to take an image of the person using the computer.

All this information is recorded at the Agent machine, sent to the NetSupport DNA Server (using a proprietary communications protocol) and is then processed and stored in the NetSupport DNA database.

Where is the personal data stored?

NetSupport DNA is an on-premise solution and runs on servers located at the school. The data stored in NetSupport DNA is stored in an SQL server database that is either installed as part of the installation or a pre-existing SQL database server. Where sensitive data is stored in the NetSupport DNA database, this data is stored in an encrypted format. Where the SQL database server is installed as part of the NetSupport DNA installation, any direct access to the database is restricted by the security policies built into the Microsoft SQL Server. Where a pre-existing SQL server is used, the access is controlled by the security policy in place for the pre-existing SQL server.

WHAT DATA IS COLLECTED AND STORED?

The table below lists all of the personal information that is stored in the on-premise NetSupport DNA database.

Name	Purpose	Legal Grounds	Sensitivity	Collection
Name	Identification	Public task / Legitimate interests*	Personal Data	**Automatically collected**
Logon Name	Identification	Public task / Legitimate interests*	Personal Data	**Automatically collected**
Email Address	Communication	Public task / Legitimate interests*	Personal Data	**Optional data**
Phone Number	Communication	Public task / Legitimate interests*	Personal Data	**Optional data**
Mobile Phone Number	Communication	Public task / Legitimate interests*	Personal Data	**Optional data**
Pager Number	Communication	Public task / Legitimate interests*	Personal Data	**Optional data**
Department	Identification	Public task / Legitimate interests*	Personal Data	**Optional data**
Employee/Student No	Identification	Public task / Legitimate interests*	Personal Data	**Optional data**
Address	Communication	Public task / Legitimate interests*	Personal Data	**Optional data**
Typed Phrases	Safeguarding	Public task / Legitimate interests*	Sensitive Data	**Automatically Collected****
Screen Capture	Safeguarding	Public task / Legitimate interests*	Sensitive Data	**Automatically collected**
Webcam Image	Safeguarding	Public task / Legitimate interests*	Sensitive Data	**Automatically collected**
Accessed URL	Safeguarding	Public task / Legitimate interests*	Personal Data	**Automatically collected**
Title of Accessed URL	Safeguarding	Public task / Legitimate interests*	Personal Data	**Automatically collected**

* The Lawful Basis for processing is decided by the Data Controller (the customer) and not by NetSupport. This table gives the suggested basis is for public authorities/companies and other organisations respectively. Please confirm with your Data Protection Officer/Data Protection lead as to the correct Lawful Basis.

**Safeguarding data is automatically collected and recorded when configured to do so. This can be applied at a granular level, but once in place the process is automatic. Resultant records would be reviewed by humans before any decisions are made, and any priority of action/risk rating can be reconfigured to act as set out by the school.

NetSupport DNA and the GDPR data subject rights

The GDPR defines eight rights of the individual with regard to the processing of personal data. Part of complying with the new regulations is to ensure that you can meet the terms of these individual rights. In this section, we explain each right and how it affects the NetSupport DNA product.

THE RIGHT TO BE INFORMED

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. For further information and guidance see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

NetSupport DNA has an “Acceptable Use Policy” feature, and we recommend that as part of your Acceptable Use Policy, you should either notify users that they are being monitored and what data isbeing recorded or direct them to your privacy policy that should contain this information.

THE RIGHT OF ACCESS

Under GDPR, individuals have the right to access their personal data. This allows individuals to be aware of and verify the lawfulness of the processing.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-of-access/

With a data subject access request, NetSupport DNA provides an export facility in the database maintenance tool that can be used to export the required data.

THE RIGHT TO RECTIFICATION

Under Article 16 of the GDPR, individuals have the right to have inaccurate personal data rectified. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-to-rectification/

The NetSupport DNA Agent installed on all computers has a feature available so that any user can view and update their personal information. Alternatively, this information can be updated manually by using the NetSupport DNA Console application.

THE RIGHT TO ERASURE

Under Article 17 of the GDPR, individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances. For information on when this right is applicable, see the ICO guidance at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

If this is applicable, then using the database maintenance feature from the NetSupport DNA Console, you can delete all the information related to an individual.

THE RIGHT TO RESTRICT PROCESSING

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. The right is not absolute, however. In most cases, you will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-to-restrict-processing/

The data that NetSupport DNA collects automatically is defined by the setting for the profile that is active when the user is logged onto a computer. If you need to disable any collection of data for an individual, you can create a profile and disable all data collection; this profile can then be assigned to an individual to stop NetSupport DNA collecting any information.

THE RIGHT TO DATA PORTABILITY

The right to data portability only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-to-data-portability/

This is unlikely to apply to any data processed by NetSupport DNA.

THE RIGHT TO OBJECT

The guidance from the ICO states that individuals must have an objection on 'grounds relating to his or her particular situation'. And that you must stop processing the personal data unless 'you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual'.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-to-object/

In the case of NetSupport DNA's eSafety and safeguarding features, this would be classed as compelling legitimate grounds for processing.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

NetSupport DNA does not perform any decision-making based solely on automated processing.

SOME COMMON QUESTIONS

IS NETSUPPORT THE DATA PROCESSOR OR THE DATA CONTROLLER?

For a customer using NetSupport DNA, NetSupport does not have access to any school's data. Once the product is installed, all of the data is stored locally on the school's servers. Therefore, within the context of NetSupport DNA, NetSupport is neither the data controller nor the data processor.

IS THE SCHOOL THE DATA PROCESSOR OR THE DATA CONTROLLER WITHIN THE CONTEXT OF NETSUPPORT SYSTEMS?

For users of NetSupport DNA, schools remain the data controller of their own data on the system.

DOES NETSUPPORT DNA PROCESS PERSONAL DATA?

Personal information associated with individual students and staff is processed by NetSupport DNA,therefore the rules of the GDPR apply to its use. This personal data is stored locally on the school's servers and therefore the school will remain the data controller and the data processor of this personal information.

DOES NETSUPPORT DNA PROCESS SENSITIVE DATA?

When an eSafety alert is triggered in NetSupport DNA, the system can be configured to record screen data and record images from a webcam. Due to the possible nature of this data, it could contain sensitive data, and as such, we recommend that this data be assumed as sensitive data.

DO I NEED TO GET CONSENT FROM ALL STAFF AND PUPILS BEFORE I CAN MONITOR THEM IN SCHOOL WITH NETSUPPORT DNA?

Generally, no – you do, however, need to give a clear notification that there is a monitoring system in place. This notification should explain that NetSupport DNA will record what they type and do, so staff and pupils understand what is monitored for safeguarding purposes. Schools should very clearly state why it is necessary to monitor students' access (and, where applicable, that of staff) and how that data will be processed, stored and deleted.

WHAT IF A CHILD/PARENT DOESN'T CONSENT TO THEM BEING MONITORED IN SCHOOL?

As above, consent is generally not required. It is important to explain the need to monitor children in school and the reasons why. The ICO gives guidance on the lawful basis for processing information. See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful- basis-for-processing/

The reasons will be a combination of public task (for maintained schools), legitimate interests (for independent schools) and the school's legal or contractual obligations, including child safety.

If you have any further questions regarding this document or any other queries regarding NetSupport DNA, please contact us:

General enquiries	**Sales enquiries**	**Technical Support**
+44(0)1778 382270	+44(0)1778 382270	+44(0)1778 382272
press@netsupportsoftware.com	sales@netsupportsoftware.com	support@netsupportsoftware.com