Information Security Policy

Date Published	**June 2016**
Version	**5**
Last Approved Date	**March 2021**
Review Cycle	**1 Year**
Review Date	**March 2022**

"Learning together; to be the best we can be"

1. Purpose

1.1. The purpose of this document is to provide a documented record of requirements for Information Assurance

1.2. It is the responsibility of Nexus Multi Academy Trust to ensure that:-

- Confidential information is protected from unauthorised access or disclosure;
- Information is accessible and available;
- Integrity of information is maintained.
- Information held by the Trust is protected from threats, whether internal, external, deliberate or accidental.
- Contractual, regulatory, audit and legislative requirements are met. Including, but not limited to:
  - Freedom of Information
  - Data Protection Act
  - Computer Misuse Act
  - General Data Protection Regulation
- All employees, volunteers, governors, consultants, contractors and agents employed by the Trust provided with authorised access to the Trust's equipment are aware of information security issues and good practice.
- All breaches of information security, actual or suspected are reported, investigated, reviewed and acted upon.

2. Review

2.1. The policy will be subject to regular review by the Trust Board and will be amended as appropriate in response to changing organisational, legislative, environmental and technical requirements.

3. Scope

3.1. The Information Security Policy shall apply to:

- All constituent academies and services in Nexus MAT;
- All permanent and temporary employees, volunteers, governors, consultants, contractors and agents employed by the Trust and provided with authorised access to the Trust's equipment, systems, information and paper records;
- All Trust Owned and/or controlled electronic equipment including desktop PC's, mobile devices and communication equipment;
- All Trust owned documents and records and those records stored by the Trust.

4. Roles & Responsibilities

4.1. The Trust Board will, either directly or through delegated powers:

- maintain and review the information security policy;
- review security incidents and take appropriate action in conjunction with HR.

4.2. The Trust Chief Executive Officer will, either directly or through delegated powers:

- Provide the necessary technical security to the Trust's ICT infrastructure;
- Maintain the technical estate through patching and maintenance;
- Ensure provision of technical knowledge on the security of equipment;
- Ensure that there is advice for system owners on the technical security of their equipment and end of life;
- Record, Monitor and report on security breaches;
- Ensure that systems are scanned to maintain and prevent security risks from malicious threats, i.e. Malware, spyware;

- Ensure that licensing agreements for software are monitored and maintained;
- Assess, record and mitigate electronic Information Assurance risks and issues.

4.3. Headteachers will ensure:

- employees receive instructions in relation to information governance during their induction, which will include data protection, information security, e-safety, records management and freedom of information;
- that the integrity of potential employees will be verified wherever possible by taking up references and carrying out vetting procedures where applicable;
- that adequate training is available for employees;
- review security incidents and take appropriate action in conjunction with the Chief Executive Officer.

4.4. Each academy system or application used by the Trust shall have a designated ICT system administrator.

5. Access to Systems

5.1. Asset Control – Personal Responsibility

5.1.1. Nexus Multi Academy Trust purchases assets for the express use of executing Trust business. These assets are assigned individually and recorded centrally by school business managers.

5.2. Returning assets

5.2.1. If assigned equipment is no longer in use by the assigned owner, it is their responsibility to return that equipment to their system administrator or line manager for the transfer/removal of personal responsibility, who will then inform the school business manager to update the academy inventory.

5.2.2. Laptops and other mobile devices shall not be stored in lockers, drawers or elsewhere as 'spares'.

5.3. User ID - Network Unique User Identification

5.3.1. All users are provided with a unique User ID to access the academy network. No attempt shall be made to sign on to any system or database using someone else's User ID. This is a security breach and should be reported to the Headteacher.

5.4. Vetting and References

5.4.1. In order to ensure that employees are reliable and trustworthy in the handling of information, references should be obtained and identity / background checks completed in accordance with Trust policy.

5.4.2. All Trust employees must have a basic security check to allow them to work. This ensures employees can legally work in the UK.

5.5. Codes of Conduct

5.5.1. Employees and Governors and volunteers must adhere to the Employee Code of Conduct which details obligations regarding disclosure of information, use of ICT and data security, use of systems and equipment and confidentiality.

5.6. Termination Of Employment

5.6.1. On leaving the employment of the Trust, all equipment & software must be returned to academy office.

5.6.2. All Trust assets remain the property of the estate and must be returned when an employee leaves the Trust.

5.6.3. The Trust will take the necessary action to reclaim all equipment, software and information that has not been returned by the member of staff (e.g. by means of final salary payment).

5.6.4. For damage limitation for the Trust, and user rights, employees formally give rights to access and handle all user data stored in "my documents". A all user data should be freely accessed by the Trust to ensure continuity of business has been identified with the leaver prior to the termination date.

5.7. Temporary Staff, Consultants and Agency Staff

5.7.1. Where staff are employed who won't go through the normal induction procedure, Headteachers/managers must ensure they are made aware of this policy and their responsibilities regarding information governance and confidentiality.

5.8. Work Experience and Student Placements

5.8.1. Students and academy children on work experience must sign a confidentiality at the commencement of their time with the Trust.

5.9. Line of Business Applications User Identification

5.9.1. Some of the Trust's applications have additional layers of security to ensure that employees only access the information that they require to carry out their duties.

5.9.2. Attempting to access another user's account on any of these systems is a security breach and should be reported to the service desk.

5.10. Emergency Access

5.10.1. Should access be required to system accounts in periods of absence, or after an employee has left the Trust, the appropriate access must be sought via the Headteacher to ensure the control of access to systems and data as per the Data Protection Act.

5.11. Authorisation Levels

5.11.1. Employees must have the information they need to do their job. Some data within Systems is segregated into levels/accounts to protect the information held within them. Authorisation levels must

be set on a need to know basis, i.e. each user shall access, only what they need for work purposes.

5.12. Password Policy

5.12.1. Access to Trust systems require a password. The requirements for that password are controlled centrally by group policy in order to meet industry guidelines and at the recommendation of CESG to ensure the security of information.

5.13. Use of the Internet

5.13.1. Internet usage must comply with the Trust's Electronic Communications Policy and you are not permitted to access websites containing adult material, paedophilia or information relating to drugs, gambling, racism, terrorism, violence or weapons (unless you have been authorised for specific work purposes).

5.13.2. The Internet must not be used for personal business, trading or share dealing.

5.13.3. Use of email is recorded and is monitored at all times.

5.13.4. Trust equipment must not be used to download and store copyrighted material, music files and videos. This is illegal and may result in disciplinary action. Regular monitoring and reporting on this takes place.

5.14. Use of E-Mail

5.14.1. Email must be used in accordance with the Trust's Electronic Communication Policy.

5.14.2. Official email shall not be used for registration to Non Work Related (NWR) good or services.

5.14.3. The content of electronic mail messages are regarded as a form of publication and are subject to libel laws. Messages must not have any

content which could be considered as defamation, harassment or discrimination.

5.14.4. Information in emails may be accessible to the public under the Freedom of Information and Data Protection Acts. Ensure that all emails are accurate, justified and professionally worded.

5.14.5. E-mail is unique to each employee. You must not allow anyone else to use this user ID. If someone else is to administer e-mails for you, you must use the delegate facility.

5.14.6. The 'Out of Office' facility must be used for any planned absence.

5.14.7. Use of internet (web- based) e-mail accounts (such as Hotmail, gmail etc.) are restricted to users who put forward a valid business case. Contact the Headteacher or your line manager for further details.

5.14.8. Access to social media sites, (Facebook, twitter etc) are restricted to users who put forward a valid business case.

5.14.9. Use the standard academy signature for all work e-mails. This should be in the following format:

Name
Job title
Academy name
Academy address
Academy contact number
Academy web address

5.15. Monitoring

5.15.1. All systems must be monitored and audited for administrative, legislative and management purposes, therefore, personal privacy cannot be guaranteed.

5.15.2. It may be necessary to access systems and equipment during an employee's absence to ensure business continuity. Please see para 5.6.4 for more information.

5.16. Security Incidents

5.16.1. All actual or suspected breaches of security and / or the information security policy must be reported in accordance with the policy:

5.16.2. Security incidents are detected by multiple different mechanisms:

- Though Trust personnel or a direct report from an end user;
- Via HR or Audit, this could be from a confidential report, management request, scheduled audit etc;
- Automated detection from content filtering or anti-virus software.

5.17. Where there is an information security breach, academies and the central Trust team will be required to complete the form in appendix c.

6. Legal, Contractual and Regulatory Requirements

6.1. Data Protection Act

6.1.1. All employees should bear in mind that the loss or misuse of personal data can be judged an offence under the Data Protection Act. You must process information in accordance with the Data Protection Policy Statement.

6.2. General Data Protection Regulation

6.2.1. The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR 2018 places more emphasis on being accountable for and transparent about your lawful basis for processing.

6.3. Freedom of Information Act

6.3.1. The Freedom of Information Act gives a general right of access to information held by the Trust. More information can be accessed in rhe Trust's Information Governance Policy

6.4. Copyright, Designs and Patents Act

6.4.1. Copyright gives the creators of original literary or artistic material a property right in the material. Literature, art, music, sound recordings, films and broadcasts and computer programs are all protected by copyright. You must ensure that you process information and use electronic files in accordance with copyright requirements.

6.4.2. Most music and video files are protected by copyright. Please ensure that any music or video used in a work context is properly licensed.

6.5. Intellectual Property

6.5.1. Any digital information, code etc that is produced by the Trust, or on their behalf, remains the intellectual property of Nexus Multi Academy trust. Removing, copying or re-producing Nexus intellectual property may result in disciplinary or legal action.

6.6. Computer Misuse Act

6.6.1. The Computer Misuse Act (1990) makes it an offence to:

- Access computer material without the permission of the system owner. This includes accessing information where you have legitimate access to a computer system but you access information you don't need to access to do your job.
- Access computer material without permission with intent to commit further criminal offences
- Alter computer material without permission e.g. writing a virus to destroy someone else's data

6.7. Software Licensing

6.7.1. Any software installed must be properly licensed. Please note that "freeware", "shareware" and "trial copies" are normally not free for

commercial use. If in doubt, please contact the academy or Trust system administrator for advice, as the library of software within the Trust may already cover your requirements.

7. Secure Storage of Data and Information

7.1. Clear Desk and Screen Policy

7.1.1. Unattended computer terminals must be turned off or locked.

7.1.2. Paper and Electronic records must be stored in accordance with the Trust's Records Management policy.

7.1.3. The GDPR requires you to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act).

7.1.4. However, the GDPR 2018 provides more specifics about what you have to do about the security of your processing and how you should assess your information risk and put appropriate security measures in place. Whilst these are broadly equivalent to what was considered good and best practice under the 1998 Act, they are now a legal requirement.

7.2. Storage of Electronic Information

7.2.1. Information pertaining to work shall be stored on the academy file server (i.e. the network, not on the computer's hard disc (C:\ Drive). Information shared to C:\ Drive is not backed up and may be accessible if equipment is lost or stolen.

7.2.2. The use of Microsoft One Drive within Office 365 is not to be used as a replacement for the user's home drive. Data stored within this area of Office 365 is not supported by the trust and staff should be aware that this area is not backed up. Whereby staff need to access their home drive and or other network drives when working off site, they should use the Trusts VPN solution.

7.2.3. The Use of Microsoft Teams is permitted for use for all staff within each school and central trust employees. The trust has provisioned each school with its own secure environment which can be used as a non-

sensitive data repository to support home workers and or those without School issued equipment.

The following key parameters of use applies to all staff;

In relation to GDPR/Data protection 2018, The following two data types should be considered at all times by team owners and its members and provide the basis of what data types are appropriate to use/store within the team environment;

Personal data -The GDPR/DPA 2018 applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive personal data -The GDPR/DPA 2018 refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

With this is mind, is it expected that sensitive personal data will **not** be stored or transmitted within the team's environment without the approval of the Trusts Data protection officer.

Personal data that pertains to a staff or students **must** be considered and would be at the discretion of the Head Teacher (School data controller) and where additional clarifications are required, Trusts Data Protection Officer.

Operational data types such as Trust/School policies, planning, risk assessments, leave charts, lesson plans, timetables and other similar documents **would** be appropriate to store and transmit within the Teams environment.

7.3. Transferring & Sharing Information and Data

7.3.1. It is important to consider the impact of data lost or stolen as a result of transporting media and also to ensure that information regularly shared is done so securely.

7.4. Information Sharing Protocols

7.4.1. Where information is shared with other organisations on a regular basis, an information sharing protocol should be in place, detailing what information will be shared, for what purpose, how it is shared etc.

7.5. Contract Clauses

7.5.1. All contract documentation should contain clauses relating to data protection, confidentiality of information and freedom of information.

7.6. Using information in non-school environments

7.6.1. Information which is classed as PROTECTED or above (refer to Appendix B for definitions) should not be discussed in a public area or where it can be overheard.

7.6.2. Do not display information which is classed as PROTECTED or above (refer to Appendix B for definitions) on your laptop or on paperwork in a public place.

7.6.3. Keep usage to a minimum in public areas due to the threat of 'overlooking' and / or theft.

7.6.4. Any member of staff choosing to use information and/or devices in public areas that results in any security breach will be required to state why the usage was necessary and the steps they took to protect the information and / or equipment.

7.6.5. Equipment in use must not be left unattended at any time.

7.7. Usage in Areas not generally accessible to the Public (inc other school premises)

7.7.1. Employees are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

7.7.2. If equipment is being used outside of its normal location and might be left unattended, the user must secure it by other means (e.g. security cable).

7.8. Home Usage

7.8.1. Information which is classed as PROTECTED or above (refer to Appendix A for definitions) must not be shared with unauthorised individuals. Only authorised members of staff are allowed access to information being used at home in any form, on any media. No

unauthorised individuals shall be allowed access to the equipment or information.

7.8.2. Information which is classed as PROTECTED or above (refer to Appendix A for definitions) must not be stored on non-Trust IT equipment. UNPROTECTED documents, such as policies or non-sensitive reports may be worked on but deleted after use.

7.8.3. Information which is classed as PROTECTED or above (refer to Appendix A for definitions) must be neatly filed and stored away when not in use. It must be stored in a locked container (filing cabinet, lockable briefcase).

7.8.4. When Files or Equipment are stored at home they should not be openly accessible to other members of the household or visible from outside the premises.

7.9. Transporting Information

7.9.1. You must only remove files and equipment from the workplace where there is a business need to do so and they should be returned as soon as possible.

7.9.2. Keep equipment secure, clean and out of sight during transit e.g.in a car boot.

7.9.3. Where a courier service is used to transport packages containing sensitive information, tamper proof packaging must be used. Ensure equipment and documentation is adequately packaged in transit to prevent damage or tampering, or loss of contents. Transport paperwork, CDs etc in a closed bag or file.

7.10. Email

7.10.1. Within the Trust, it is safe to email files. However, sensitive data should be password protected and/or encrypted. Advice can be provided by the academy or Trust system administrator.

7.10.2. Information which is classed as PROTECTED or above (refer to Appendix A for definitions) must not be sent to or from home via personal email as the information is not secure.

7.10.3. All electronic transfer of data must be transported in a secure manner. Information which is classed as PROTECTED or above (refer to Appendix B for definitions) must not be transferred outside the Trust using plain email, CD/DVD or USB stick without encryption.

7.10.4. All data transfer classified at PROTECTED or above, between the Trust and other Public Services (Local Authority/Central Government departments etc) should be done using secure mail or following protocols.

7.10.5. Please contact the academy or Trust ICT system administrator for instructions on how to securely email data.

7.11. Removable media

7.11.1. Only Trust provided memory drives, also known as memory sticks, USB drives and USB pens, shall be used to TRANSFER data.

7.11.2. Memory drives shall not be used to STORE data, the Trust shall provide appropriate systems to store data safely and securely.

7.12. Use of Telephones, Mobile phones, Fax Machines and Printers

7.12.1. Telephones and fax machines must be used in accordance with the electronic communications policy.

8. Accessing Information from Outside the UK

8.1. The Data Protection Act states that information cannot be transferred out of the European Economic Area (EEA) unless specific security safeguards are established. Therefore information must not be transferred overseas without suitable safeguards. When using Trust ICT equipment overseas, you must ensure that information is only accessed via the Trust network and is not downloaded, in order to ensure that an overseas transfer does not take place.

8.2. Accessing mobile networks from outside the UK carries higher risks and should only be considered in an emergency.

8.3. The Trusts email platform, Office 365, is not accessible outside of the UK by default. This is in line with the principles of "protection by design" as set out by the General Data Protection Regulation 2018.

Staff members that have a "directed" operational need to access their nexusmat.org email account whilst outside of the UK should contact their Head Teacher to request access.
This request should include the required duration of access and from what country and purpose of access.
The Head Teacher will then contact the Trusts Data Protection Office (Mr Warren Carratt) to seek approval.

9. Acquisition of Computer Equipment

9.1. Advice must be sought from the academy or Trust system administrator before new systems, hardware or software is acquired to ensure the ongoing compatibility with the network and operating systems.

9.2. All new hardware must be purchased, imaged and asset tagged prior to introduction to the academy/Trust network to ensure the continued security of the network.

9.3. Equipment purchased outside this mandate will not be allowed on the Trust/academy network to ensure its' continued security.

10. Disposal of Data and Information

10.1. Confidential Waste

10.1.1. Documents containing information which is classed as PROTECTED or above (refer to Appendix A for definitions) must be disposed of via the academy confidential waste system.

10.2. Disposal of IT Equipment

10.2.1. Disposal of computer equipment must be via the academy/Trust system administrator.

10.3. Protection Against Malicious Code

10.3.1. All desktop and server hosts are equipped with Symantec Anti-virus with End-Point Protection. Virus definitions are updated in-line with best practise, upon release.

10.3.2. The email gateway only allows certain approved file-types to be allowed entry to the network.

10.3.3. Firewall hardware checks and prohibits malicious code it detects on incoming web traffic and email.

10.4. Network Controls

10.4.1. The academy's network perimeter is protected by firewalls and anti-virus software.

10.5. Wireless Network

10.5.1. The wireless LANs are AES \ WPA2 encrypted to the highest industry standard. Trust staff access a specific wireless network which is completely separate from any public wireless networks.

Appendix A – Data Classification Definitions

Nexus Multi Academy Trust ("the Trust") as a private registered company remains compliant with legacy Data Classifications.

Data Type	Impact if the data is lost or stolen and misused	Examples
UNRESTRICTED	None / negligible	Information published on the Trust or academy Web Sites or is otherwise publicly available Information that would be disclosed in response to a Freedom of Information Request Disclosure will not adversely affect a client or member of staff
PROTECTED	inconvenience to pupils or families damage to the Trust's standing or reputation	Personal data relating to any client or member of staff such as a name, address or any personal identifier Any other data considered to be covered by the Data Protection Act Any data which may result in financial loss Any data which is considered to be commercially or politically sensitive
RESTRICTED	substantial inconvenience or distress significant impact to a pupil or families substantial damage to the Trust's standing or reputation	A complete client record containing many personal details Volumes of "PROTECTED" data about a large number (10+) of pupils or staff

	prejudice the investigation of or facilitate the commission of crime could have wider implications for the Trust's finances or reputation	
CONFIDENTIAL	prejudice to the safety security or liberty of an individual impede the investigation or facilitate the commission of serious crime could have major implications for the Trust's finances or reputation	A large number of complete pupil records A set of data relating to many pupils or staff which in combination could result in harm to those individuals

Appendix B - PC Disposal Policies and Procedures

Any equipment that can be reused by the Trust will be reused.

Any equipment that cannot be will be securely disposed of in the following ways:

Where hardware is **intact but with parts that could be reused by a manufacturer**, there is a marginal resale value. The Trust will sell these items. Before computers are passed to the third party we will run 'secure delete' routines on the hard drives.

Where hardware is **intact but totally beyond use**, the WEEE directive compels manufactures to agree to dispose of any equipment that they have supplied to the Trust since July 2005. In this scenario the academy will deliver the equipment to a pre-agreed collection point. The supplier will then dispose of or recycle the equipment in a way that complies with the relevant legislation.

Where hardware is **not intact** we will contract with a third party to dispose of this equipment for us. The third party will dismantle the equipment and recycle all recyclable components. Hard drives will be securely destroyed, precious metals will be recovered and toxic substances safely disposed of.

There are several other issues which we must consider in order that we comply with the WEEE directive:

- **Storage Sites** – all old equipment is stored in secure rooms prior to disposal.
- **Transfer** – we require that carriers are licensed and have been checked in accordance with the requisite Waste Management legislation. We will operate a compliant system of transfer and consignment notes. Third parties will be supplied with a list of tag numbers before they arrive and we will be issued with receipts detailing all equipment that has been collected.
- **Disposal Sites** – we require that the disposal sites have the appropriate waste management licences and procedures in place.

IT Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Headline Information for this Incident	
Nature of incident (Cyber, Non Cyber or both):	
Affected site(s)	
Date incident started:	
Date reported/identified:	
Has root cause of the incident been confirmed?	
Date resolved:	

2. Incident Description
Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.
☐ Loss / Compromise of Data
☐ Damage to Systems
☐ System Downtime
☐ Financial Loss
☐ Other Organisations' Systems Affected

☐Damage to the Integrity or Delivery of Critical Goods, Services or Information ☐Violation of legislation / regulation ☐Unknown at this time
Provide a brief description:

4. Sensitivity of Data/Information Involved

Has the incident resulted in a loss of integrity, authenticity or confidentially of stored, transmitted or processed data? ☐ Yes ☐No	
If yes, then please confirm which type of data:	
☐Public data (i.e. date which could be released under FOI into the public domain) ☐Internal Use Only	☐Restricted / Confidential (Privacy violation) ☐Unknown / Other – please describe:
Provide a brief description of data that was compromised:	

5. Who Else Has Been Notified? (Note - This must include the named Data Protection Office

Provide Name(s) and Designation(s):
If personal data has been breached, has this been reported to the ICO under the GDPR? ☐ Yes ☐ No ☐Not applicable

6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.	
☐No action taken ☐System Disconnected from network ☐Updated virus definitions & scanned system	☐Restored backup from tape ☐Log files examined (saved & secured) ☐Other – please describe:
Provide a brief description:	

7. Further Incident Details	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are non-Nexus systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Form Completed by:	
Designation:	
Date:	

A copy of this form must be submitted to the Trust's named Data Protection Officer, who in turn will ensure this is shared with Directors/Trustees.

A copy should also be submitted to the responsible Data Controller, if the incident has happened at an academy.