Information Security Policy (Non Statutory)

NUNTHORPE MULTI ACADEMY TRUST

Preamble

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Nunthorpe Multi Academy Trust's (NMAT's) programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Information Security Policy outlines NMAT's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 270001 (internationally recognised information Security standard).

This policy should be read in conjunction with the other policies in NMAT's Information Governance policy framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

Scope

All policies in the Information Governance policy framework apply to all NMAT employees, any authorised agents working on behalf of NMAT, including temporary or agency employees, and third party contractors.

Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card. (The use of USB devices is discouraged by the Trust and their use will be phased out over the next 12 months),
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images. NMAT employees, authorised agents and third party contractors must not use their own devices to take photographs or other digital images.

Access Control

NMAT will maintain control over access to the personal data that it processes.

These controls will differ depending on the format of the data and the status of the individual accessing the data. NMAT will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). In terms of IT, this log will be maintained by IT Network manager in each Academy. In terms of data relating to Child Protection, this log will be maintained by the Designated Safeguarding Lead in each academy. For SEND data this will be maintained by the SENDCO in each NMAT academy.

Manual Filing Systems
Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be locked in a safe place. The IT Network Manager, Designated Safeguarding Lead and SENDCO will be responsible for giving individuals access to the relevant key. Access will only be given to individuals who require it to carry out legitimate business functions.

Electronic Systems
Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two tier authentication system will be implemented across all electronic systems. The two tiers will be username and unique password.

Individuals will be required to change their password every 60 – 90 days and user names will be suspended either when an individual is on long term absence or when an individual leaves employment of NMAT.

Software and Systems Audit Logs
NMAT will ensure that all software and systems have inbuilt audit logs so that NMAT can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

External Access
On occasions NMAT will need to allow individuals who are not employees of the Trust to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another Academy. The relevant Head of School is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access then access can also be authorised by the Vice Principal and/or the Executive Principal.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the academy's IT Network Manager.

Third-Party Data Hosting
It is necessary for the trust to use third party data processors. However, NMAT only uses companies that comply with all applicable GDPR provisions as defined by the General Data Protection Regulation EU 2016/679 ("GDPR"). Any data exported from a third-party hosting services, and digitally stored externally from an NMAT site, must be either encrypted and/or anonymised.

Physical Security

NMAT will maintain high standards of physical security to prevent unauthorised access to personal data. The following controls will be maintained by each Academy in the Trust:

Clear Desk Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable facilities to secure personal data when not in use.

Alarm System
NMAT and each Academy will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. NMAT Health & Safety and site teams will be responsible for authorising key distribution and the IT Network manager (Nunthorpe Academy) and the Site Manager (Rye Hills Academy) will maintain a log of key holders.

Internal Access
Internal areas that are off limits to pupils and parents will be kept locked and only accessed through key fobs.

Visitor Control
Visitors to the academies will be required to sign in via the electronic signing in system and state their name, organisation, car registration (if applicable) and nature of business. Visitors will be escorted throughout the academy and will not be allowed to access restricted areas without employee supervision.

If appropriate, visitor books (electronic and paper based) will be locked away at the end of the working day and kept for current financial year + six years.

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, NMAT must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of NMAT but NMAT will implement the following mitigating controls in line with Business Continuity Plans.

Information Security Policy (Non Statutory)

Back Ups
NMAT academies will back up their electronic data and systems regularly and the frequency is determined by the criticalness of the systems**.** These backups will be kept in a different part of the building and where possible in a different building. This arrangement will be governed by a data processing agreement. Should the Academy's electronic systems be compromised by an environmental or natural hazard then the Academy will be able to reinstate the data from the backup with minimal destruction.

Fire Proof Cabinets
The Academy will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises. Where practicable, data is increasingly being stored on clouds.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System
The Academy will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems Security

As well as physical security NMAT also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect NMAT's ability to operate and could potentially endanger the lives of its students.

NMAT will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions
Employees must request authorisation from the IT team before downloading software on to the Academy's IT systems. The IT team will vet software to confirm its security certificate and ensure the software is not malicious. The IT team will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Phishing Emails
In order to avoid computer systems from being compromised through phishing emails, employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the IT team they are unsure about the validity of an email.

Information Security Policy (Non Statutory)

Firewalls and Anti-Virus Software
NMAT requires that firewalls/web filters/antivirus and security software that needs to be installed on any applicable electronic devices, will be the latest stable version to achieve maximum protection. Firewalls/ web filters are regularly assessed to ensure they provide the best security for the academies in the Trust.

Shared Drives
NMAT Academies maintains a shared drive on their servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. For example, a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The ICT team at each Academy will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the Academy's retention schedule.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the Trust and students alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. NMAT has implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by post
When sending personal data, excluding special category data, by post, each Academy will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post
When sending special category data by post each NMAT Academy will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Exceptional Circumstances
In exceptional circumstance NMAT may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function
When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then NMAT employees will utilise the Blind Copy (BCC) function.

Information Security Policy (Non Statutory)

NUNTHORPE MULTI ACADEMY TRUST

Surveillance Security

The academies in the Trust operate CCTV at its premises.

Due to the sensitivity of information that could collected as a result of this operation, NMAT has a separate policy which governs the use of CCTV software. This policy has been written in accordance with the ICO's Surveillance Code of Practice.

Remote Working

It is understood that on some occasion employees of NMAT will need to work at home or away from the Academy premises. If this is the case then the employees will adhere to the following controls:

Lockable Storage
If employees are working at home they will ensure that they have lockable storage to keep personal data and NMAT equipment safe from loss or theft. Employees must not keep personal data or Academy equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).
Employees must not keep personal data or NMAT equipment in cars if unsupervised.

Trusted Wi-Fi Connections
Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from the ICT team.

Password protected devices, encrypted devices and Email Accounts
Employees will only use NMAT issued password protected, where practicable encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a Trust issued device.

Employees will not use personal email accounts to access or transmit personal data. Employees must only use NMAT issued, or NMAT authorised, email accounts.

Data Removal and Return
Employees will only take personal data away from the NMAT premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to NMAT premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.