OFFICIAL POLICY FOR

NMAT INFORMATION SECURITY INCIDENT REPORTING POLICY (Non-Statutory)

Preamble

From May 2018 the UK's existing Data Protection Act was replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Nunthorpe Multi Academy Trust's (NMAT) preparation for this new legislation, a new information policy has been developed.

This policy has been written to govern the Trust's management of information security incidents and data breaches.

Glossary

NMAT Specific Point of Contact (SPOC) - NMAT HR, Compliance and Data Protection Lead.

NMAT external Data Protection Officer – Veritau.

Senior Information Risk Owner (SIRO) – Executive Principal, Head of School or member of the academy's Senior Leadership Team as applicable.

Information Asset Owner (IAO) – Person identified by the Trust as the 'process' Owner from whichever process the breach has occurred.

Queries about any aspect of NMAT's Information Governance strategy or corresponding policies should be directed to the Specific Point of Contact (SPOC) who is the NMAT HR, Compliance and Data Protection Lead in the first instance. This is done via DataProtection@nmat.co.uk or queries can be sent to the external Data Protection Officer at SchoolsDPO@veritau.co.uk

Scope

This policy applies to all NMAT employees, any authorised agents working on behalf of NMAT, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They 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;
- 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.

Article 33 of the GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore, it is vital that NMAT has a robust system in place to manage, contain, and report such incidents. The Information Security Incident Management Policy details how NMAT will handle and manage information security incidents when they arise.

Notification and Containment

In order for NMAT to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain, and report such incidents.

Immediate Actions (Within 24 Hours)

If an employee, Trustee, Governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the SPOC (see above) within 24 hours. If the NMAT Data Protection Lead is not at work at the time the email auto-forwarding facility will nominate another individual to start the investigation process.

If appropriate, the individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the SPOC will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings can be found in Appendix One of this document.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The SPOC will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams if applicable.

Reporting to the ICO/Data Subjects (Within 72 Hours)

The SIRO, in conjunction with the relevant manager, SPOC, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The relevant manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents

The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the School.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

Appendix 1 Severity Rating Threshold

Rating	Incident Threshold	Recommended Actions
WHITE **Information Security Event**	No breach of confidentiality, integrity, or availability has taken place but there is a failure of the implemented safeguards that could lead to a breach in the future. *Examples* ▪ A post-it note containing a user name and password to a Trust database is found attached to a keyboard. ▪ A key safe, containing keys to filing cabinets, has been found unlocked and unsupervised.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on Data Protection Software.
GREEN **Minimal Impact Incident**	The Trust's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Incident has been contained within the organisation (or trusted partner organisation). The information does not contain any special category data or any data that would be considered to be sensitive. The actual or potential detriment to individuals is virtually non-existent. *Examples* ▪ An email, containing details of a service user's address or contact details, is sent to an incorrect recipient within the Trust. ▪ A document containing the only record of pupil's contact details have been destroyed in error.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on Data Protection Software. ▪ Notify SIRO. ▪ Investigation report to be conducted by Information Asset Owner.
AMBER **Moderate Impact Incident**	The Trust's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left Trust control. The information does not contain special category data or data that is considered to be sensitive but may contain data that should have been confidential to the Trust. The incident appears to affect only a small number of individuals.	▪ Responsible officer(s) asked to re-sit Data Protection e-learning. Management to consider HR action. ▪ Consider utilising key messages/intranet to remind all staff of certain data protection best practice. ▪ Logged on Data Protection Software.

Appendix 1 Severity Rating Threshold

	The actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioner's Office. *Examples* ▪ A letter is sent to the wrong postal address and the incorrect recipient has learnt of another individual's dealings with the Trust. However, the letter does not contain any special category information. ▪ An email has been sent to ten parents without the BCC function being utilised which reveals all ten personal email addresses.	▪ Notify SIRO. ▪ Investigation report to be conducted by Information Asset Owner.
RED **Serious Impact Incident**	The Trust's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left Trust control. The information contains special category data or data that is considered to be sensitive in nature and/or affects a large number of individuals. The incident has or is likely to infringe on the rights and freedoms of an individual and has a likely potential to cause detriment (emotional, financial, or physical damage) to individuals. *Examples* ▪ A file, containing safeguarding and health data, is left unsupervised in a vehicle which is subsequently stolen and the data has been lost to persons unknown. ▪ A spreadsheet containing the SEN information for all the Trust's pupils has been mistakenly sent to a member of the public.	▪ Management to consider (potentially immediate) HR action. ▪ Logged on Data Protection Software. ▪ Notify SIRO and Data Protection Officer. ▪ Consider reporting to the Information Commissioner's Office. ▪ Consider informing affected individual(s). ▪ Consider informing the police or other law enforcement agencies. ▪ Where appropriate the Data Protection Officer to conduct incident investigation with assistance (where and if required) from internal audit and counter fraud colleagues.