Information Security Incident Reporting Policy

Date Published	**June 2016**
Version	**4**
Last Approved Date	**March 2021**
Review Cycle	**1 Year**
Review Date	**March 2022**

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

1. Introduction

1.1. Nexus Multi Academy Trust has a legal obligation to ensure the security of all its assets, i.e. equipment, software and information in any format.

1.2. In order to fulfil these obligations, the Trust must implement a system to report and record breaches in security, carry out investigations, ensure appropriate actions are taken and implement measures to prevent further incidents recurring.

1.3. Principle 7 of the Data Protection Act (1998) requires the Trust to take appropriate measures against unauthorised and unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data. Article 5 of the General Data Protection Act (2018) strengthens this putting a duty on data processors to ensure "appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

1.4. The failure to identify and report security incidents such as unauthorised access, use or misuse of IT equipment, software or information could result in:

- The loss of IT equipment, software or information
- The processing of incomplete or corrupted data
- Repeated unauthorised access, use or misuse and/or fraudulent activity
- Action not being taken to correct control or systems weaknesses
- Distress and/or damage to the Trust's stakeholders potentially resulting in legal action and/or financial penalties
- Loss of customer confidence

2. Scope

2.1. This policy relates to all academies and settings across Nexus MAT and supersedes any local policies and procedures that have been in use prior to the academy conversion.

3. Aims of the Policy

3.1. The aims of this policy are to:

- Ensure compliance with all legal requirements on the Trust;
- Identify the actions required to ensure that all incidents are recorded, investigated and reported to senior management and that security arrangements are reviewed and amended to prevent further incidents
- Provides guidelines as to what constitutes a breach
- Ensure all Trust governors, staff and volunteers are aware of their responsibilities regarding security incidents

4. Scope of the Policy

4.1. This policy will identify the controls to be implemented to ensure the full management of security incidents.

4.2. The policy applies to all governors, staff, volunteers and any third parties who have authorised access to the Trust network and / or information.

4.3. An information security incident is any incident resulting in the loss (or potential loss) of information, misuse of information, unauthorised destruction or alteration of information (whether deliberate or accidental), disclosure of information to an unauthorised person, integrity of systems or data being compromised, or disruption to information processing systems.

5. Responsibilities

5.1. Governors, staff and volunteers are responsible for:

- Reporting any actual or suspected security breach;
- Obtaining prior authorisation for items / issues that might otherwise be identified as a security breach, for example, loading non-Trust software onto a PC;

5.2. Managers will be responsible for:

- Making all staff, partner agencies and contractors aware of the reporting procedures;
- Reporting serious incidents to Senior Leaders;
- Investigating incidents;
- Recommending any action required to prevent breaches.

5.3. HR will take all necessary disciplinary action regarding reported incidents.

6. Guidelines for Reporting

6.1. NOTE: All parties must bear in mind that accessing IT equipment, software or data to investigate a security incident, could result in corruption of evidence rendering it unusable for use in a disciplinary or criminal action at a later date. Further advice can be sought from the Trust/academy ICT Administrator.

6.2. All information security incidents must be reported to the Headteacher in their capacity as Data Controller who will inform the Chief Executive Officer of the Trust, the named Data Protection Officer and record the details and action taken on the form at Appendix A.

6.3. Where incidents are reported to HR services by staff, HR will pass details to the Headteacher (anonymised where necessary) in order for the details to be recorded and to identify common security issues, training needs, changes to policies etc.

6.4. If there are significant losses of personal information, the named Data Protection Officer will inform the Information Commissioner's Office, where appropriate.

Appendix 1 – Incident Report Form

Section 1 - Incident Details	
Incident Detected By: Name: Title: Contact Details: Date Detected: Time Detected:	**Incident Location:** Academy: department:
Staff Details: Name: Title: Contact Details: Line Manager:	**Incident Type:** Loss of information Inappropriate Material Child Protection Issue Harassment Misuse of Equipment/Information Deliberate Unauthorised Disclosure Other breach of IS/E-Comms or DP Policy Fraud Misuse of Financial Systems Other (provide details): _____ _____ _____ _____ _____ _____

Appendix 1 – Incident Report Form

Further Details (more detailed description of incident):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Appendix 1 – Incident Report Form

Section 2 – Action Taken	
Action Taken: _____ _____ _____ _____ _____ _____ _____ Taken By: Time: Date Result: _____ _____ _____ _____ _____ _____ _____	**Action Taken:** _____ _____ _____ _____ _____ _____ _____ Taken By: Time: Date Result: _____ _____ _____ _____ _____ _____ _____
Action Taken: _____ _____	**Action Taken:** _____ _____

Appendix 1 – Incident Report Form

_____ _____ _____ _____ _____ Taken By: Time: Date Result: _____ _____ _____ _____ _____ _____ _____ _____	_____ _____ _____ _____ _____ Taken By: Time: Date Result: _____ _____ _____ _____ _____ _____ _____ _____

Section 3 – Incident Review

Incident Cause: Procedural Human Error Lack of Awareness of Policies/Procedures	**Was it preventable:** Yes/No **What could have prevented the incident:** _____

Appendix 1 – Incident Report Form

Malicious Intent Other (provide details): _____ _____	_____ _____
Issues Raised: Training needs: _____ _____ _____ Policy changes required: _____ _____ _____ Technical changes required: _____ _____ _____ Other changes required: _____ _____ _____	