

Our Lady of Mercy Catholic Education Trust



St Anthony's Girls' Catholic Academy

Policy type:	M.A.T.
Policy:	Data Breach Policy 2018-2019
Ratified by MAT Directors:	December 2018
Head Teacher signature:	<i>M. Shepherd.</i>
Chair of Directors signature:	<i>Shepherd.</i>
Review Date:	December 2019
Ownership:	M.Shepherd (Head Teacher)

1.0 Introduction.

1.1 The academy's Data Breach Policy has been produced to ensure compliance with the Data Protection Act 2018 (DPA), GDPR and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO) and is in line with our academy ethos which aims for excellence in all aspects of our work.

1.2 St. Anthony's Girls' Catholic Academy holds processes and shares personal data that needs to be protected.

1.3 Every care is taken to protection personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.4 Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, detrimental effect on service provisions, legislative non- compliance, and /or financial costs.

2.0 Purpose.

2.1 St. Anthony's Girls' Catholic Academy is obliged under the Data Protection Act and the General Data Protection Regulation to have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the school/academy.

3.0 Scope.

3.1 This policy relates to all personal and special category data held by the school/academy regardless of format.

3.2 This policy applies to all staff and pupils and contractors at the school/academy. This also includes student teachers, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school/academy.

3.3 The object of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

4.0 Types of breach.

4.1 For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the academy's information assets and/or reputation.

4.3 An incident includes, but is not restricted to, the following:

- loss or theft of confidential or special category data or equipment on which such data is stored e.g loss of a laptop, memory stick, i-pad/tablet or a paper record,
- equipment theft or failure,
- un-authorized use of, access to or modification of data or information systems,
- attempts (failed or successful) to gain unauthorised access to information or I.C.T. systems,
- un-authorized disclosure of special category confidential data,
- website defacement,
- a hacking attack,
- unforeseen circumstances eg. fire or flood,
- human error.
- blagging offences ie. where information is obtained by deceiving the organisation who holds it.
- Near misses

5.0 Reporting an incident.

5.1 Any individual who accesses, uses or manages the academy's data is responsible for reporting data breach and information security incidents

immediately to the Head Teacher/Academy Business Manager who will immediately inform the Data Protection Officer.

5.3 If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. N.B. the academy has 72 hours to report a breach to the Information Commissioner.

5.4 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many people are involved. An incident reporting form will be completed as part of the reporting process.

6.0 Containment and recovery.

6.1 The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach. This will depend on the nature of the breach. In certain situations this may be the DPO.

6.3 The Lead Investigation Officer (LIO), from the Senior Leadership Team (SLT) of the academy, will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.5 The LIO, in liaison with the relevant officers determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and risk assessment.

7.1 An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being discovered/reported.

7.2 The LIO will investigate the breach and assess the risks associated with

it, for example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to take into account the following:

- . the type of data involved,
- . it's sensitivity,
- . the protection in place e.g encryption,
- . what has happened to the data ie. has it been lost or stolen,
- . whether the data could be put to illegal or inappropriate use
- . who the individuals are, the number affected and the potential effects on those data subjects,
- . whether there are wider consequences to the breach.

8.0 Notification.

8.1 The DPO will determine whether the breach needs to be reported to the Information Commissioner.

8.2 Every incident will be assessed on a case by case basis. However, the following will be considered:

- . whether there are any legal/contractual notification requirements,
- . whether notification would assist the individual affected - could they act on information to mitigate the risks,
- . whether notification would help prevent the unauthorised or unlawful use of personal data,
- . would notification help the school/academy meet its obligation under the principle,
- . whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they

can contact the school/academy for further information or to ask questions about what has occurred.

The LIO and/or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. The LIO and or DPO will consider whether any press release may be required. All actions will be recorded by the LIO and DPO.

9.0 Evaluation and response

9.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 This review will consider:

- where and how the personal data is held and where it is stored,
- where the biggest risks lie and identification of any further potential weak points within its existing measures,
- whether methods of transmission are secure and sharing minimum amount of data necessary,
- identifying weak points within existing security measures,
- staff awareness,
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

10.0 Policy Responsibility

10.1 The person with overall responsibility for this policy is the Head Teacher.