St Maryof the Angels

Data Incident
Guidance and Policy Framework

Data Protection - Data Breach Procedure for St Mary of the Angels

Policy Statement

St Mary of the Angels holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by St Mary of the Angels and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at St Mary of the Angels if a data protection breach takes place.

1.0 Legal Context

St Mary of the Angels will comply with the requirements of Article 33 of the General Data Protection Regulations in relation to the Notification of a personal data breach to the supervisory authority

1.1. In the case of a personal data breach, the controller (the school) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1.2. The processor shall notify the controller (the school) without undue delay after becoming aware of a personal data breach.

1.3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1.4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

1.5. The controller (the school) shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action

taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

2.0 Types of Breach

2.1. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

3.0 Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

3.1 The person who discovers/receives a report of a breach must inform the Head Teacher, the schools Data Protection Lead or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. This should be done by completing the attached breach notification form.

3.2. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3.3. The DPO (or nominated representative) must inform the Head/Chair of Governors as soon as possible if the breach is considered of a serious nature. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

3.4. The DPO (or nominated representative) must also consider whether the Police need to be informed. 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. In such instances, advice from the School's legal support should be obtained.

3.5 The DPO will take the decision based on the severity of a breach and the likely effect on data subjects as to whether the ICO should be notified (this should occur within 72 hours of the incident being identified) and to whether the data subject should be notified.

3.5. The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant Council Department, so that they are prepared for any potentially inappropriate enquiries for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

c. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation Process

1.0 Investigation

1.1 In most cases, the DPO to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

1.2 A clear record should be made of the nature of the breach and the actions taken to mitigate it.

1.3 The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office.

1.4 A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

2.0 Notification

2.1 Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place.

2.2 The DPO (or nominated representative) should decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

2.3 When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

3.0 Review and Evaluation

3.1 Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it.

3.2 It should be reported to the next available Senior Management Team and Full Governors meeting for discussion.

3.3.If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right.

3.4 If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

3.5 This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

4.0 Implementation

4.1 The /DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training.

4.2 If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

School Information Security Incident Reporting Form

Completed forms must be sent as soon as possible to *Tracy Mills, School Data protection Lead*

Provide as much information as you can, but do not delay sending in the form, incidents must be notified within 24 hours of identification.

GENERAL DETAILS	
Incident number:	*To be assigned by data protection lead*
Reported by:	*Named member of staff*
Date of incident:	*When did it occur*
Date incident was identified:	*When was it identified*
Reported Date:	*Date DPO/DP Lead/Head Notified*
Location of incident :	*In school, offsite etc*

ABOUT THE INCIDENT – provide as much information as possible.	
Incident description. Please describe the incident in as much detail as possible	
How did the incident occur?	*Provide as much known information as possible*
When did the incident happen?	*If no accurate date can be identified, be approximate*
How was the incident identified?	*Was it discovered by the school, reported by a parent/3rd party*
What personal data has been placed at risk?	*Details of information you believe may have been*
In what format was the information involved?	*Letter, email, USB pen etc.*
Was the data encrypted/appropriately secured?	*Was secure email used, was USB secure, if system access what controls were in place*
Dealing with the current incident	
Has the school taken any immediate action to minimise/mitigate the effect on the affected individuals?	*If so, provide details.*
How many individuals have been affected?	*Number of pupils, staff, parents etc. who may have been affected by information being put at risk*

Have any affected individuals complained to the school about the incident?	*Have they complained direct, have they referenced complaining to the ICO?*
What are the potential consequences and adverse effects on those individuals? (parents, pupils or staff)	*Don't just think worst case scenario, think of any consequences to individuals even if it is merely 'inconvenience'*
Has the data subject been informed/is the data subject aware?	*Have they already been told or are they likely to be aware e.g. parents talking to each other, was it reported in the press etc.*
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.	*Can you verify the risk has been removed – the data recovered or destroyed, vulnerabilities addressed etc.*
Preventing a recurrence	
Has any action been taken to prevent recurrence?	*What steps have been taken – policies, procedures, change in working practice, training etc.*
Are further actions planned? If so, what?	*Have other actions been scheduled, e.g. an audit of processes, training etc.*
Who has the action been agreed by?	*Has any action been signed off by Head, Governors, DPO etc.*
Individuals Involved	
Have the staff involved in the security incident done any Data Protection Training?	*Document what training was carried out*
If so, what and when? (Please list)	*Document when any/last training was carried out*
How long have those involved worked at the School?	*Addresses whether training is required for new staff*
Are the staff involved: agency staff, new starters, part time staff, full time staff etc?	*Addresses whether training is required for different levels of staff, governors etc.*

	IMPACT ASSESSMENT QUESTIONS	
1.	**Was any data lost or compromised in the incident?** E.g. Loss of an encrypted item should not actually have compromised any information	Yes/No
2.	**Was personal data lost or compromised?** This is data about living individuals such as pupil, staff, parents etc.	Yes/No
3.	**If yes, was <u>sensitive</u> personal data compromised?** This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, philosophical beliefs, potential or actual criminal offences, genetic or biometric data.	Yes/No
4.	**Does any of the information lost or compromised relate directly to a child/children?**	Yes/No
5.	**Was safeguarding, child protection or health data involved?**	Yes/No

6.	**What is the number of people whose data was affected by the incident?**	
7.	**Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals? Physically, materially, or morally?** Example - physical harm, fraud, reputation, financial loss, distress	Yes/No
8.	**Did this incident involve information belonging to another organisation?** e.g. NHS, Local Council, Police etc.	Yes/ No
9.	**Did people affected by the incident give the information to the School in confidence?** (i.e. with an expectation that it would be kept confidential)	Yes/No
10.	**Is there a risk that the incident could lead to direct damage to any individual** e.g. via identity theft/ fraud/impersonation?	Yes/No
11.	**Could the incident damage an individual's reputation, or cause hurt, distress, embarrassment or humiliation** e.g. loss of medical records, disciplinary records etc.?	Yes/No
12.	**Can the incident have a serious impact on the School's reputation?**	Yes/No
13.	**Has any similar incident happened before?**	Yes/No
14.	**Was the school aware such an incident was possible or likely to occur?**	Yes/No

REVIEW: to be completed by Data Protection Lead/Data Protection Officer (where required)	
Incident Number:	
Classification:	[ ] Breach [ ] Incident [ ] Offence
Principles identified as breached:	1) Lawful, fair and transparent
	2) Specific, explicit and legitimate purposes
	3) Adequate, relevant and limited to what is necessary for processing.
	4) Accurate and kept up to date
	5) Kept in a form that allows for the identification of data subjects only as long as necessary
	6) Processed in manner that ensures its security.

Is a full investigation required?	
Have data subjects been informed?	
Have key stakeholders (Parents, Governors, Local Authority etc) been informed?	
Have control weaknesses been highlighted and recommendations made?	
Has sufficient and appropriate action been taken?	
Does the incident need reporting to the DPO?	
Does the incident need reporting to the ICO?	
Has the Incident Log been updated?	
Further investigation undertaken by:-	
Notes: **(Reasons for referral/non-referral to ICO)**	

Sign off and Outcomes		
Item	**Name/Date**	**Notes**
Measures to be implemented approved by:		*Responsibility for actions and required completion date – school DP Lead/Head*
DPO advice and recommendation provided:		*DPO advice in relation to mitigating risk, action to be taken*
Summary of DPO Advice:		
DPO Advice accepted or overruled by:		*If overruled, reason must be stated and by whom*
Comments:		
Date Closed:		

Breach Reporting Log

Incident Number	Date of Incident	Incident Type	Identified Breach	Identified Cause	Number of individuals affected	Full Investigation	Data Subjects Informed	ICO Informed	Action Taken
			• Confidentiality • Integrity • Availability • Accountability	• Human error • System failure • etc		Yes/No Link to full report if yes	Yes/No (date)	Yes/No (date)	Disciplinary action etc
0001/2018	1/2/18	Letters sent to incorrect recipients	Confidentiality	Human Error	15	No	No but aware	No	Procedure for the production and handing out of letters to class pupils to ensure staff members checks as to correct recipients.