St Mary's
Catholic Primary School and Nursery

SECURITY INCIDENT AND DATA BREACH PROCEDURE

Guidance

It is important that staff are fully aware of the School's data incident procedure in relation to reporting a data breach.

A data breach extends to include information that is at a risk of a loss and is not restricted to an actual loss of information.

St Mary's will immediately inform the Data Protection Officer of the breach/incident. The DPO has a legal responsibility to assess the seriousness of any incident and report serious occurrences to the Information Commissioner's Office within 72 hours.

Details as to how to report a breach is available on the website www.stmaryscrewe.co.uk in order for parents/carers to understand the procedure and raise concerns.

Policy Statement

St Mary's Catholic Primary School & Nursery holds large amounts of personal and sensitive data. We take every care to protect personal data and to avoid a data protection breach. In the event of data being lost/shared inappropriately, it is vital that we take the appropriate action to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by St Mary's and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action that all staff follow if a data protection breach takes place.

Legal Context

St Mary's 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. 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. This does not apply if 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 has not made within the 72 hours period, the reasons for the delay is included with the notification.

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

3. The notification referred to in point 1 above shall, as a minimum:

- 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
- Communicate the name and contact details of the Data Protection Officer or other contact point where more information is available
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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.

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. Please see the Data Breach Notification form.

Types of Breach

Data protection breaches can occur from a number of factors including but not restricted to the following examples, whether accidental or unlawful:

- 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
- Disclosure or being made available where it should not have been
- Made available to unauthorised persons

Managing a Data Breach

Where St Mary's is aware of a personal data breach, the following steps are taken:

- The person who discovers/receives a report of a breach must complete a Data Breach Notification form and inform the Headteacher, the Data Protection Lead or the Data Protection Officer (DPO). Where the breach occurs or discovered outside normal working hours, the reporting should commence as soon as is practicable.

- The DPO (or nominated representative) must ascertain whether the breach continues to occur and immediately take steps 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.

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

- The DPO (or nominated representative) must also consider whether to notify the Police of the breach. This would be appropriate where there has been illegal activity, there may have been illegal activity or where there is a risk that illegal activity might occur in the future. In such instances, contact Cheshire East Legal Services for further advice.

- 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 whether the data subject should be notified. To decide this, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality

- Any other significant economic or social disadvantage to the individual(s) concerned

- The DPO will notify the ICO via the 'report a breach' page of the ICO website within 72 hours of the incident being identified. he DPO will provide:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If any of the above information is unknown, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

1. Attempting to recover lost equipment.

2. Contacting the relevant department. This will ensure that they are prepared for any potentially inappropriate enquiries for additional information on the individual or individuals concerned. A global email to all school staff may be considered. If an inappropriate enquiry is received, the enquirer's name and contact details should be taken with confirmation that their call will be returned. The enquiry must be reported immediately to the Headteacher/DPO (or nominated representative).

3. Back-ups will restore lost/damaged/stolen data.

4. If bank details have been lost/stolen, contact the bank directly for advice on preventing fraudulent use.

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

Investigation

In most cases, the DPO will fully investigate the breach. The DPO (or nominated representative) will ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps are required to remedy the situation. The investigation will include:

- the type of data
- the sensitivity of the data
- 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
- the type of people who have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

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

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

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

Notification

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO normally makes the decision to notify individuals or agencies once an initial investigation has taken place.

The DPO (or nominated representative) should decide who 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.

When notifying individuals, specific, clear and concise advice will be given detailing how they can protect themselves and how St Mary's can help them. We will also give the individual an 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, what data was involved and what the measures taken to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the DPO (or nominated representative) will review the causes of the breach and the effectiveness of the response to it. All actions will be documented and retained within the School Business Managers office.

The breach will be reported to the next available Senior Leadership Team meeting and Full Governing Body meeting for discussion.

If systemic or ongoing problems are identified, then an action plan must be drawn up to remove the problem.

If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.
This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

St Mary's will ensure that all staff are aware of the School's Data Protection policy and its requirements including this breach procedure. The implementation forms part of the induction process and ongoing training.

Staff should discuss any queries in relation to the School's Data Protection Policy and associated procedures with their Team Leader, DPO Lead or the Headteacher.

St Mary's
Catholic Primary School and Nursery

DATA BREACH NOTIFICATION

Please return completed forms to the Data Protection Lead (Mrs Lisa Lee).

Please provide as much information as you can, but do not delay sending in the form; please notify the potential breach within 24 hours of identification.

GENERAL DETAILS	
Incident number: *(assigned by Data Protection Lead)*	
Reported by:	
Date of incident:	
Date incident was identified:	
Reported Date: **DP Lead** **Headteacher** **DPO**	
Location of incident :	
ABOUT THE INCIDENT *(provide as much information as possible)*	
INCIDENT DESCRIPTION	
How did the incident occur?	
When did the incident happen? *(If no accurate date can be identified, be approximate)*	
Who identified the incident?	
What personal data is at risk?	
What was the format of the information?	
Was the data encrypted or appropriately secured? *(secure email, encrypted USB, if system access what controls were in place)*	
DEALING WITH THE CURRENT INCIDENT	
What immediate action was taken to minimise/mitigate the effect on the affected individuals?	
How many individuals are affected?	

Have any affected individuals complained to the school about the incident?	
What are the potential consequences and adverse effects on those individuals?	
Has the data subject been informed or 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, provide details of how and when this occurred.	
PREVENTING A RECURRENCE	
What action has been taken to prevent recurrence?	
Are further actions planned? If so, what?	
Who has the action been agreed by?	
INDIVIDUALS INVOLVED	
Have the staff involved in the security incident done any Data Protection Training?	
If so, what and when? (Please list)	
How long have those involved worked at the School?	
Are the staff involved: agency staff, new starters, part time staff, full time staff 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>likely</u> to result in a <u>risk</u> to the individual/individuals?**	Yes/No
8.	**If yes to question 7, is the risk:** **Physical harm** **Material harm** **Moral harm** *Example - physical harm, fraud, reputation, financial loss, distress*	 Yes/No Yes/No Yes/No
9.	**Did this incident involve information belonging to another organisation?** *e.g. NHS, Local Council, Police etc. If so, which organisations?*	Yes/ No
10.	**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
11.	**Is there a risk that the incident could lead to direct damage to any individual** *e.g. via identity theft/ fraud/impersonation?*	Yes/No
12.	**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
13.	**Can the incident have a serious impact on the School's reputation?**	Yes/No
14.	**Has any similar incident happened before?**	Yes/No
15.	**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?	Yes/No
Have data subjects been informed?	Yes/No
Have key stakeholders (Parents, Governors, Local Authority etc) been informed?	Yes/No
Have control weaknesses been highlighted and recommendations made?	Yes/No
Has sufficient and appropriate action been taken?	Yes/No
Does the incident need reporting to the DPO?	Yes/No
Does the incident need reporting to the ICO?	Yes/No
Has the Incident Log been updated?	Yes/No

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:		

St Mary's
Catholic Primary School and Nursery

BREACH REPORTING LOG

Incident Number	Incident Date	Incident Details	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 • Other (specify)		Yes/No (Link to full report if yes)	Yes/No (and date)	Yes/No (and date)	Changes in policies and procedures, Disciplinary action etc.