ST JOSEPH'S CATHOLIC PRIMARY SCHOOL
DATA BREACH PROCEDURE AND INCIDENT REPORT FORM

Revision History

Version	*Revision Date*	*Revised by*	*Section Revised*
V1.2	13th June 2018	Julie Galvin	Whole Document
V2	5th July 2018	Julie Galvin	Whole Document

Document Control

Document Owner:	***Document No:***	***Status:*** Draft/Approved	***Date Approved:***
Security Classification: High/Medium/Low	***Next Review Date:***	***Version:*** V2	***Department:***

1. Data Breach Procedure

This procedure is written using guidance from the ICO (Information Commissioner's Office), www.ico.org.uk

These guidelines must be followed to ensure that any breach or potential breach is dealt with in accordance with legislation and with the support of our Data Protection Officer (DPO)

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Manager who will then start the incident process and notify the Data Protection Officer.
- The DPO will investigate the report, and determine whether a breach has occurred. The DPO will consider if personal data has been accidently or unlawfully:

    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPM will alert the Headteacher and the Chair of Governors
- The DPM/DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant members of staff or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. The DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (e.g key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically with restricted access.

- Where the ICO must be notified, the DPO will do this via the 'Report a Breach' page at www.ico.org.uk within 72 hours. As required the DPO will set out:
    - 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 the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- 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:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure that it does not happen again (such as establishing more robust processes or providing further staff training)

Records of all breaches will be stored electronically and with restricted access.

- The DPO and the Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as is reasonably possible.

Data Protection Manager :

Mr P Murton
St Joseph's Catholic Primary School
155, Aldershot Road
Guildford
Surrey
GU2 8YH
dpm@stjosephsguildford.com

Data Protection Officer :

Kristy Gouldsmith, Sapphire Consulting
07545 501220
dpo@stjosephsguildford.com

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL

DATA BREACH INCIDENT FORM

DPO/DPM:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
DDI:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO OF DATA SUBJECTS AFFECTED:		**NO OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			

PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?		**YES/NO**	
IF YES, WAS THIS WITHIN 72 HOURS?		**YES/NO/NA**	
If no to the above, provide reason(s) for delay			
IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?		**YES**	**NO**
A description of the nature of the personal data breach			
The categories and approximate number of data subjects affected			
The categories and approximate number of personal data records concerned			
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)			
A description of the likely consequences of the personal data breach			
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)			
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?		**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:			
DETAILS OF INCIDENT INVESTIGATION:			
PROCEDURE/S REVISED DUE TO BREACH:			

STAFF TRAINING PROVIDED: *(if applicable)*	
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:	
HAVE THE MITIGATING ACTIONS PRVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*	
WERE APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE?	**YES/NO**
If yes to the above, describe measures	

Investigator Signature: _____ Date: _____

Investigator Name: _____ Authorised by: _____