Policy for

GDPR Policy:

Breach and Non-Compliance Policy

23/24

Document Control

A. Confidentiality Notice	This policy document has been approved by the Governing Body of St Modwen's Catholic Primary School and is intended for internal and/or external publication. Where the document is identified for internal use the policy information may not be shared with external agencies or parents without the prior agreement of the Headteacher or authorizing committee.			
B. Document Details	**Classification:**	Premises, Health and Safety Committee		
	Policy Source:	John Walker (Data Protection Officer) May 2023 Version		
	Organisation:	St Modwen's Catholic Primary School		
	Documents reference:	Policy number: STM47		
	Current Version Number:	V1(6 pages)		
	Current Document Approved by: (Committee)	PH&S		
	Date Approved:	Autumn 2 Term 2023		
	Statutory Policy	Yes		
	Internal/External Policy (published on website)	External – Publish on website		
	Schedule Review:	**Next Review date:**	**Review cycle**	
		Autumn Term 2 2024	Annually	

C. Version Control Document revision and Approval History	**Version**	**Date**	**Version created by:**	**Version approved by:**	**Comments**
	V1	7.11.2023	School	PH & S	Revised August 2023 – John Walker Policy 12.5.2023 refresh **Amends:** 5. GDPR Linked policies p5

D. Contents	Section	Page No
	1. Personal data breach procedure	2-3
	2. Actions to minimise the impact of data breaches	4
	3. Data Processing	4
	4. Review process	4
	5. GDPR related policies	5
	Appendix 1: Data Breach and Non- Compliance Log	6

1. Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) completing the reporting form on GoGDPR portal.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (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 on the school's computer system, and GoGDPR portal.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored school's computer system, and GoGDPR portal.

The DPO and Headteacher/School Business Manager will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

- The DPO and Headteacher/School Business Manager will meet Termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

2.0 Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

SENSITIVE INFORMATION BEING DISCLOSED VIA EMAIL (INCLUDING SAFEGUARDING RECORDS)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Details of pupil premium interventions for named children being published on the school website

Non-anonymised pupil exam results or staff pay information being shared with governors

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

The school's cashless payment provider being hacked and parents' financial details stolen

Hardcopy reports sent to the wrong pupils or families

3. Review

A review of the effectiveness of school Breach and Non-Compliance processes will be conducted by the School Business Manager every 12 months.

4. Data Processing

Data will be processed to be in line with the requirements and protections set out in the UK General Data Protection Regulation.

5. GDPR Related Policies and Procedures

	Review Date
01 Data Protection Policy	September 2024
02 Breach and Non-Compliance Policy	September 2024
03 Confidentiality Policy and Confidential Agreements	September 2024
04 CCTV Policy	September 2024
05 Workforce Acceptable use Policy	September 2024
06 Freedom of Information Policy	September 2024
07 Document and Data Retention Policy	September 2024
08 Privacy Notices: • Pupils Data • School Trips • Staff Workforce • Governors • Job Applicants • PTA • External School Photographer	September 2024
09 GDPR Workforce and Governor Training/CPD • GDPR Guidelines for staff	September 2024
10 GDPR Checks, Compliance and Audit Toolkit (GoGDPR)	September 2024
11 GDPR Subject Access Request Management and Procedures	September 2024
12 GDPR My rights a guide for data subjects	September 2024
13 GDPR Home School Communication Charter	September 2024
14 GDPR Information Security Protocol	September 2024
15 Cyber Response Plan	September 2024

Appendix 1: Data Breach and Non- Compliance Log

Data Breach and Non Compliance Log												
Date	**Description of breach**	**Categories of data affected**	**Categories of individuals affected**	**Cause of the breach**	**Effects**	**Reported to the ICO?**	**Why/why not?**	**Were individuals informed?**	**Action taken to contain the breach**	**Date the breach was reviewed**	**Actions taken to stop the breach happening again**	**Additional notes**