ST. PETER'S CATHOLIC PRIMARY SCHOOL

SECURITY AND DATA BREACH POLICY

If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time. Please consult the Policies page on the website for the latest update.

Controlled Document

Title	**Security Incident and Data Breach Policy**
Document Type	Approved
Author	Data Protection Enterprise Ltd
Owner	Headteacher
Document Version	Version 2
Created	August 2023
Approved by	Board of Governors
Review Date	31/08/2026 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control

Version	Date	Author	Description of Change
1	20/01/2022	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	New Policy
2	23/08/2023	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Policy Review

Contents:

1. INTRODUCTION

The School are aware of its responsibilities under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 to ensure appropriate and proportionate security of the personal data the school holds.

Every care must be taken to protect information and to avoid a security incident, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. In the unlikely event of such a security incident it is vital that appropriate action is taken to minimise any associated risk. The School will investigate all security incidents classified as 'serious' using a set plan and follow a Breach Management Plan in the event of a data breach.

Obligations and responsibilities under the UK General Data Protection Regulation are not optional; **they are mandatory**. There can be harsh penalties, up to £17.5 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to £8.7 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

All individuals permitted to access personal data in line with their work must agree to comply with this policy and agree to undertake any relevant training that may be appropriate.

2. PURPOSE

The purpose of this policy is to ensure a standardised management approach in the event of a serious security incident, including the handling of a data breach. Security incident management is the process of handling security incidents in a structured and controlled way ensuring they are dealt with:-

- speedily and efficiently
- consistently
- ensuring damage is kept to a minimum (i.e loss of equipment (laptop/memory stick) and/or loss of personal data)
- ensuring that the likelihood of recurrence is reduced by the implementation of appropriate measures.

3. SCOPE

This policy applies to all information held by the School falling within the scope of the UK General Data Protection Regulation and Data Protection Act 2018, in all formats including paper, electronic, audio, and visual. It applies to all staff and those working on behalf of the School who have access to the School's information.

This policy takes effect immediately and all staff should be made aware of security incident requirements. Any queries should be directed to the Data Protection Officer (contact details below).

4. TYPES OF SECURITY INCIDENTS

This policy addresses the reporting and handling of security incidents and data breaches.

A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored i.e. IT equipment or information (laptops, mobiles, devices containing personal data e.g. memory sticks)
- Unauthorised disclosure containing personal information
- Inappropriate access controls allowing unauthorised use
- Breach of physical building access/security
- Human error e.g. personal information being left in an insecure location, using incorrect email or postal address, uploading personal information to a website
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deception

5. REPORTING A SECURITY INCIDENT

This section explains how to report a security incident including a data breach.

5.1 The person who discovered the security incident MUST report the security incident to the Data Protection Officer immediately by email and no later than 24 hours using the security incident form (appendix A). If this is not possible then a senior staff member should be informed. If the incident occurs or is discovered outside normal working hours this should be done as soon as practicable.

5.2 The Data Protection Officer will determine and lead on an investigation although others may be invited to assist depending on the severity of the security incident. Staff must not attempt to conduct their own investigations (other than reporting the incident).

5.3 The Headteacher is ultimately responsible for making any decisions on serious security and incident breaches.

5.4 Any decision to take disciplinary action will be in line with the School's disciplinary policy.

5.5 The security incident report will be concluded when all investigations are complete.

6. RESPONSIBILITY OF A DATA PROTECTION OFFICER

Breach Management Plan

The Data Protection Officer will lead all data breach investigations and will follow the Information Commissioner suggested Breach Management Plan:-

i. Containment and Recovery
ii. Assessment of ongoing risk
iii. Notification of Breach
iv. Evaluation and Response

I. Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach including, where necessary, damage limitation.

The Data Protection Officer will:

- Lead the investigation
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a process, finding a lost piece of equipment, or simply changing access codes etc.
- Establish if there is anything that can be done to recover any losses and limit the damage the breach can cause.
- Where appropriate inform the ICO within 24 - 72 hours and;
- Where appropriate inform the police

ii. Assessing the risks

The next stage of the management plan is for the Data Protection Officer to assess the risks which may be associated with the breach considering the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

In making this assessment the Data Protection Officer will assess:

- What type of data is involved
- How sensitive it is
- If data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data
- What are the consequences if a third party has the data
- How many and who are the individuals' affected
- What harm can come to those individuals
- If there are wider consequences to consider such as a risk to public health or loss of public confidence

iii. Notification

The Data Protection Officer will decide whether the Information Commissioner or the data subjects should be notified of the breach and will inform the Headteacher. The Information Commissioner must be notified within 24 – 72 hours. This is the sole responsibility of the Data Protection Officer and staff **must not** make any notifications directly.

The Information Commissioner will need to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This will be assessed on a case by case basis by the Data Protection Officer.

iv. Evaluation and Response

The Data Protection Officer will:

- fully review both the causes of the breach and the effectiveness of the response to it
- keep a breach log
- report to the Headteacher
- implement an action plan to correct identified issues if required
- monitor staff awareness of security issues and look to fill any gaps through training

7. DATA PROTECTION OFFICER DETAILS

Data Protection Enterprise Ltd
Mobile: 07853091905
Email: info@dpenterprise.co.uk

8. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

9. LINKS WITH OTHER POLICIES

This Security Incident and Data Breach policy is linked to the School:

- Data Protection Policy
- Freedom of information Policy
- CCTV Policy
- Data Protection Impact Assessment Policy
- Acceptable Use Policy
- Information Security Policy
- Safeguarding policy

•UK GDPR Privacy Notices

The Information Commissioner also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk

Appendix A

Security Incident and Data Breach Notification Form

Contact Details of person submitting form:

Name:	
Job Title:	
Contact Number:	
Email:	

Incident Information

Date of incident?	
How did the incident happen?	
Who reported the incident?	
Description of Breach:	

Type of Breach:

Loss of IT equipment	☐	Human error	☐
Theft of IT equipment	☐	Hacking	☐
Unlawful disclosure	☐	Blagging/Phishing	☐
Unlawful access	☐	Fire/Flood	☐
Other *(please describe)*			

Personal data placed at risk

What personal data has been placed at risk? *Please specify if any financial or sensitive personal data has been affected and provide details of the extent.*

Number of Individuals affected:

Have the affected individuals been made aware: Yes ☐ No ☐

What are the potential consequences and adverse effects on those individuals?

Have any affected individuals complained about the incident? Yes ☐ No ☐

Provide details of any action taken to minimise/mitigate the effect on the data subjects.

Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

Please provide brief details of any supporting information:

Once complete please email form to: Data Protection Officer: info@dpenterprise.co.uk