The Parochial Church Council of
Saint George the Martyr, New Mills

DATA BREACH POLICY

Introduction

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. We need to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

Purpose

This policy aims to standardise our response to any reported data breach incident and ensure that they are appropriately acted upon in accordance with best practice guidelines.

Through this we hope that:

- incidents are reported and dealt with in a timely manner
- incidents are handled appropriately by the relevant people
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- the diocese is informed as required
- the incidents are reviewed to identify improvements in policies and procedures.

Scope

The policy relates to all personal data held by the Incumbent and PCC of Saint George the Martyr, New Mills, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the Church. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Responsibilities

All PCC members are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident

Any person using personal data on behalf of the Incumbent and PCC of Saint George the Martyr, New Mills is responsible for reporting data breach incidents immediately to the Incumbent and PCC Data Controller.

The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery

The Incumbent and PCC Data Controller will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Advice from the Diocese or appropriate experts will be sought if necessary. Consideration will be given as to whether the police should be informed. A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment

An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The Incumbent and PCC Data Controller will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption, password protection)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

Notification

The Incumbent and PCC Data Controller will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious.

Guidance on when and how to notify the ICO is available on their website www.ico.org.uk/media/1536/breach_reporting.pdf

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.

The Parochial Church Council will keep a record of all actions taken in respect of the breach.

Evaluation and response

Once the incident is contained, the Incumbent and PCC Data Controller, alongside the PCC will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

This policy is adapted from Christ Church Cambridge Data Breach Policy. This can be found at:
https://www.christchurchcambridge.org.uk/church-data-breach-procedure

Signed:  **(Chair of the PCC)**

Date adopted by PCC: 19th May 2024 **Review Date:** Annual APCM