PORTOBELLO AND JOPPA PARISH CHURCH

DATA BREACH PROCESS, NOTIFICATION FORM AND RETENTION PERIOD SUMMARY

Introduction

Portobello and Joppa Parish Church (the Church or the Congregation, including those acting on its behalf) collects, holds and processes personal information associated with its members and others. Simply by virtue of the organisation doing the collection, holding and processing being a church, the personal information involved can potentially be seen as information on an individual's religious beliefs and therefore by its nature could be special category personal data, subject to a greater degree of protection than ordinary personal data. The Church will hold and retain all personal information in accordance with its data protection and retention policies.

Types of breach

This document covers both confirmed and suspected incidents. In this context an incident is any incident which may compromise the confidentiality or integrity of the personal data retained by the Church. An incident includes, but is not restricted to:

- loss or theft of confidential or sensitive data or any equipment on which such data is stored (loss of laptop, USB stick, phone, tablet, paper record).
- Equipment theft or failure.
- System failure.
- Unauthorised use of, access to or modification of any such data or system.

Reporting an incident

Any person controlling any Church information who is concerned that a breach has occurred should in the first instance contact the Church office (Anne Russell, office@portyjoppachurch.co.uk), whom failing Adrian Smith (07814 785137, acnsmith80@gmail.com).

Any report should consider full and accurate details of the incident including when the breach occurred (dates and times), who is reporting it, the nature of the data involved and how many individuals it covers.

Anne and Adrian's role will be as follows:

- To determine if a breach is still occurring and, if possible, to determine what steps can be taken to minimise the effect of the breach;
- To assess the severity of the breach and whether anything can be done to recover any losses and/or limit the damage the breach could cause, taking into account for example if the information involved is encrypted and whether there are wider consequences of which to take account.

- To take any advice from any experts as may be available to help determine the severity of the incident and therefore to determine the most suitable course of action.
- To notify presbytery and/or the Data Commissioner if necessary, taking into account the dangers of over-reporting.
- To identify and if possible notify any individuals concerned. Notification will include a description of the breach and data involved and any specific/clear advice on what those individuals can do to protect themselves.
- To consider notifying third parties such as the police, insurers or banks/credit card companies.
- To make and keep a record of the incident and any lessons learned and consider whether a review of the incident to determine process improvements and/or additional training would be valuable.

Any investigation will take place immediately (within 24 hours of the breach being discovered/reported) to the extent possible.

March 2019

DATA PROTECTION BREACH NOTIFICATION FORM

If your Congregation is concerned that there has been a data protection breach, particularly in relation to information security, this form should be used. Please note that it is to be sent to your relevant Presbytery and copied to the Church of Scotland Law Department. The Church of Scotland Law Department's email address is: lawdept@churchofscotland.org.uk

DETAILS OF INDIVIDUAL REPORTING BREACH

NAME	OFFICE	TELEPHONE NO.	EMAIL ADDRESS

DETAILS OF RELEVANT PRESBYTERY

PRESBYTERY	PRESBYTERY CLERK

DETAILS OF THE DATA PROTECTION BREACH

Please enter as full information as possible in relation to the incident which you believe has resulted in a data breach. Please confirm what happened and if the incident was reported to the police.

PERSONAL DATA PLACED AT RISK

Please note all personal data you believe was located on the device you believe has been compromised. Please confirm if the documentation was password protected. Please confirm if the device was encrypted. Please confirm the number of individuals affected by the breach and whether you plan to let them know.

CONTAINMENT AND RECOVERY

If the matter has been reported to the police, please provide the name of the station it has been reported to, together with the Crime Office Reference Number, Incident and Reference Number and officer responsible. Please confirm if any CCTV is available. Please confirm if there are any witnesses to the incident.

TRAINING AND GUIDANCE

Please confirm if your Congregation/Presbytery has participated in the training provided by the Law Department, whether by attending a seminar in person or via the online webinar. Please confirm if you are aware of the GDPR resources for Congregations.

PREVIOUS CONTACT WITH THE ICO

Please confirm if you have reported any breaches previously.

MISCELLANEOUS

Please confirm any further information which would be helpful for the Data Controller/Law Department in this respect.