Personal Data Breach Record

A **"Personal Data Breach"** is any act or omission that compromises the security, confidentiality, integrity or availability of personal information (Personal Data) or the physical, technical, administrative or organisational safeguards that we as a Church have put in place to protect it. The loss, or unauthorised access, disclosure (sharing) or acquisition, of Personal Data is a Personal Data Breach e.g. emailing Personal Data to the wrong person, leaving Personal Data in a public place where others can access it or losing a laptop or USB stick.

If you know or suspect that a Personal Data Breach has occurred, immediately contact the Appropriate Controller (see Data Protection Policy) as directed by the Data Breach Policy so that they can help you to investigate the matter and take appropriate steps in line with that policy and any accompanying guidelines and procedures. Use this template to keep a record of **all** Personal Data Breaches[1]:

Details of breach						**Consequences of breach**	**Measures taken/ to be taken**		
Date of breach	No. people affected	Type of breach[2]	Description	How you became aware	Type of personal information (Personal Data)[3]		Individual informed?[4]	Remedial action	Controller informed?[4]
2.5.18	*1*	*Unauthorised disclosure*	*Mis-typed email address*	*Realised just after hitting send.*	*Contact Details*	*Possible disclosure to third party*	*No*	*Sent email asking recipient to ignore and delete email*	*No*

[1] This record is based on the *Information Commissioner Officer's (ICO) Personal Data Security Breach Log* developed in relation to the Privacy and Electronic Communications Regulation 2011 (PECR). The Appropriate Controller will notify the individuals concerned or any applicable regulator where there is a legal requirement to do so. You should preserve all evidence relating to the potential Personal Data Breach using this template.

[2] Type of breach would include; loss of Personal Data (e.g. misplaced USB stick), unauthorised access or disclosure or other breach of security (e.g. sending email to incorrect recipient), confidentiality, integrity (e.g. unauthorised person amending personal information) or availability (e.g. database down).

[3] Use types of data listed in Section 2 of the Privacy Notice.

[4] Contact the Appropriate Controller before informing individuals or contacting the ICO.
