Diocese of Arundel & Brighton

Data Breach Procedure

1 ABOUT THIS POLICY

1.1 This Policy describes the actions that must be taken by staff to report any incident which may result in a Personal Data breach. A "Personal Data breach" is defined in Article 4(12) of the General Data Protection Regulation (GDPR) as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

1.2 Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a Personal Data breach. The term "incident" is used in this Policy to describe any situation which may, upon investigation, turn out to be a Personal Data breach.

1.3 This Policy should be read in conjunction with the Diocese's Data Protection Policy which can be found on the Diocese's website.

2 IDENTIFYING AN INCIDENT

2.1 An incident may come to light in a number of ways. For example, it could occur by:

2.1.1 direct observation e.g. where a member of staff spots that Personal Data has been sent to the wrong email address;

2.1.2 being reported to us by a Data Subject: e.g. where a Data Subject notifies us that s/he has received Personal Data relating to another Data Subject;

2.1.3 being reported to us by a third party, such as a contractor, a local authority or a member of the public; or

2.1.4 an audit / review revealing that an incident had occurred.

The Arundel and Brighton Diocesan Trust is a Registered Charity no. 252878

3 ACTIONS TO TAKE ONCE AN INCIDENT HAS BEEN IDENTIFIED

3.1 Whenever an incident is identified, the following actions must be taken:

	Action	Responsibility	Timelines
1.	Report the incident to DPO via the Diocese's Chief Operating Officer.	Person who was first made aware of the incident	**Immediately after the incident is identified**
2.	Investigate and identify the full details of the incident to identify the cause	DPO for the Diocese (with the assistance of the person who reported the incident)	**As soon as possible following the incident being reported**
3.	Identify any remedial action (see paragraph 4 below)	DPO for the Diocese	**As soon as possible following the incident being reported**
4.	Complete a formal Personal Data Breach Report Form and return it to the Diocese's DPO via the Diocese's Chief Operating Officer.	DPO for the Diocese	**Within 48 hours of the incident being identified**
5.	Review the Personal Data Breach Report Form and determine whether the incident constitutes a Personal Data breach or a 'near miss' (i.e. an incident which does not meet the definition of a Personal Data breach)	DPO for the Diocese	**As soon as possible following step 4**
6.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual Data Subjects, of the Personal Data breach (see paragraph 5 below)	DPO for the Diocese	**As soon as possible following step 4**
7.	If necessary, notify the ICO of the Personal Data breach	DPO for the Diocese	**Within 72 hours of the incident being identified**
8.	If necessary, notify individual Data Subjects of the Personal Data breach	DPO for the Diocese	**Without undue delay (in practice this should be done as soon as possible)**

4 TAKING REMEDIAL ACTION

4.1 Following the reporting of the issue, the Diocese's DPO shall advise the relevant member of Diocese personnel what remedial action must be taken, in particular where parishioners, vulnerable individuals or children are affected in any way by the Personal Data breach. Individuals may suffer distress and inconvenience where they are aware that a breach has

The Arundel and Brighton Diocesan Trust is a Registered Charity no. 252878

occurred. In some cases they may be at risk of suffering financial detriment or physical harm as a result of the breach.

4.2 Remedial action should seek to mitigate any risks the individual has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the Diocese's reputation. Action will be dependent on case specifics.

If there is any doubt at all about the remedial action required to be taken, the DPO must contact the Diocese's solicitors.

4.3 Remedial action might include the following:

4.3.1 if Personal Data is in the hands of a third party, it should be retrieved from the third party or deleted from the third party's IT system (please speak to the Chief Operating Officer for assistance);

4.3.2 if the breach arose as a result of an IT issue, the source of the issue should be identified and rectified (please speak to the Chief Operating Officer for assistance); and/or

4.3.3 if the breach arose as a result of human error, the individual at fault should be made aware of the error and where appropriate asked to undertake additional training or (only in the most serious cases) be subjected to disciplinary action.

5 NOTIFYING A PERSONAL DATA BREACH

5.1 Under the GDPR, there is an obligation to report a Personal Data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of the Diocese becoming aware of the breach.

5.2 There is an exception to this reporting requirement where the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the Diocese's DPO following receipt of the Personal Data Breach Report Form; copies of which are available on the Diocese's website.

5.3 Where the Personal Data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A Personal Data breach that may result in a high risk to individuals may include where an individual is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then the Diocese's DPO must inform them of the breach by letter. The Diocese's DPO will make the final decision as to whether notifying individuals is required and what explanation is provided to them.

5.4 Where individuals are aware that they are the subject of a Personal Data breach, then they must be contacted promptly. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

5.5 Where appropriate, remedial action should also be considered for any other individuals who may also have been affected indirectly.

The Arundel and Brighton Diocesan Trust is a Registered Charity no. 252878

5.6 The Diocese's DPO will decide whether or not the affected individuals should also be sent a written apology to minimise the Diocese's reputational damage. This decision will be taken in conjunction with the Diocese' insurers.

5.7 As well as the requirement to report Personal Data breaches to the ICO, it may also be necessary to report them to other authorities such as the Police and to the Diocese's insurers. These actions should only be undertaken following consultation with the Diocese's DPO.

6 FOLLOW-UP ACTION

6.1 To ensure that we learn from our mistakes, the parish, individual or group responsible is required not only to confirm that remedial action has taken place, but also that the causes of the Personal Data breach have been analysed and action has been taken to ensure similar breaches do not occur again. Confirmation of this action will be reported and saved by the Diocese's DPO as an audit trail.

7 CENTRAL LOGGING OF THE ISSUE

7.1 Once the parish, individual or group responsible has confirmed that remedial action and any appropriate follow-up action has been taken, provided that:

7.1.1 the individual being satisfied with the remedial action taken in respect of the breach; and

7.1.2 the Diocese's DPO being satisfied that regulatory procedures have been followed;

then the breach can be marked as closed by the DPO.

7.2 A copy of all breach forms will be kept by the DPO and stored at the Diocese's registered office in Hove.

8 GLOSSARY

"**Data Controller**" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with the data protection laws including the GDPR and establishing practices and policies in line with them.

"**Data Processor**" means any person, organisation or body that Processes personal data on behalf of and on the instruction of the Diocese. Data Processors have a duty to protect the information they process by following data protection laws.

"**Data Subject**" means a living individual about whom the Diocese processes Personal Data and who can be identified from the Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data and the information that the Diocese holds about them.

"**Personal Data**" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, the Diocese's possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not

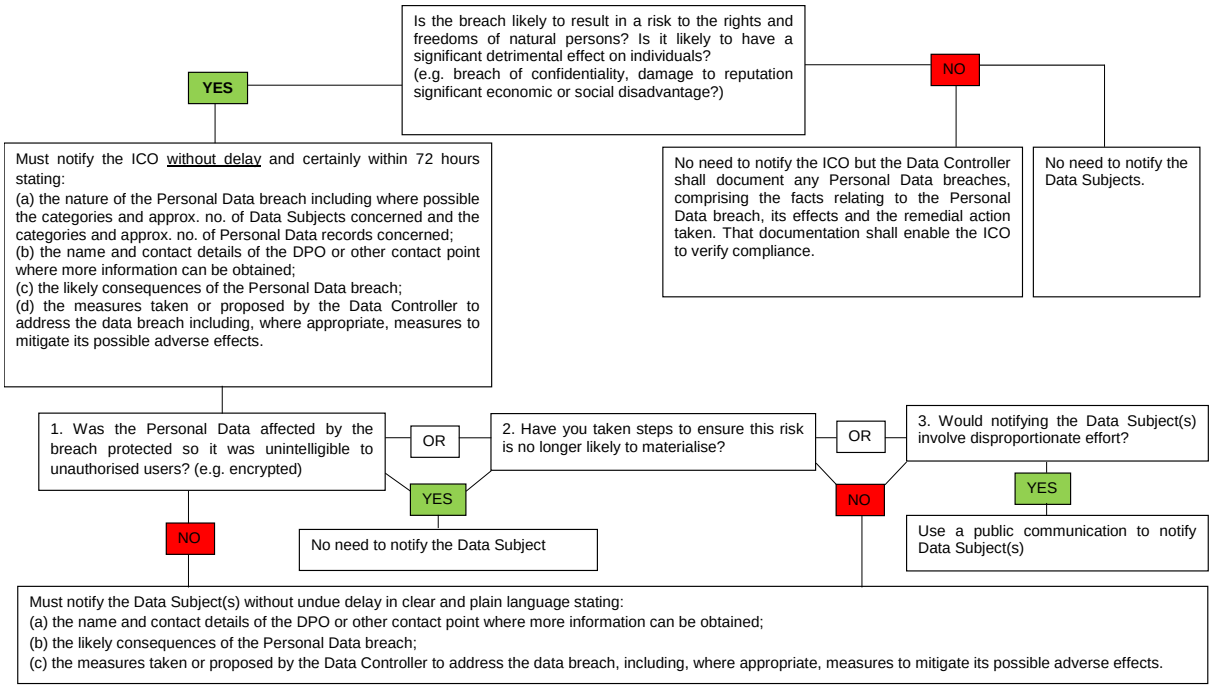
The Arundel and Brighton Diocesan Trust is a Registered Charity no. 252878

necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

"**Processing**" means any activity that involves use of Personal Data. It includes obtaining, recording or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"**Special Categories of Personal Data**" (previously called sensitive personal data) means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

DATA BREACH PROCEDURE FLOWCHART



The Arundel and Brighton Diocesan Trust is a Registered Charity no. 252878