DIOCESE OF Hexham & Newcastle

Data Breach Response Policy and Procedure

1. DEFINITIONS

1.1 **"The Diocese"** refers to the Diocese of Hexham and Newcastle including its constituent Parishes and Partnerships.

1.2 **"Diocesan personnel"** refers specifically to employees, clergy, religious and volunteers.

1.3 **"Children and young people"** in this policy are defined as anyone under the age of 18 years.

2. SCOPE

2.1 The policy is applicable to the Diocese and specifically to Diocesan personnel.

2.2 The policy should be read in conjunction with the Diocesan Data Protection Policy.

3. PURPOSE

3.1 The purpose of this policy is to have a standardised approach throughout the Diocese in the event of a Personal Data breach.

3.2 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."*

3.3 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.

3.4 A Data Breach Reporting Procedure Flowchart is included which details the actions that must be taken to report any incident which may result in a Personal Data breach.

4. ROLES AND RESPONSIBILITIES

4.1 The Chief Operating Officer (COO) has overall responsibility to ensure that all Diocesan personnel are aware of the policy, how it affects them and that they comply.

4.2 The Diocesan Data Protection Lead (DPL) is responsible for:

4.2.1 ensuring compliance of the Diocese;

4.2.2 ensuring that all those involved in an incident complete the necessary reporting procedures connected with this policy.

4.3 All employees, clergy, religious and volunteers are responsible for their action and for reporting any incidents that could result in a breach of Personal Data to the Diocese.

5. IDENTIFYING AN INCIDENT

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

5.1.1 direct observation e.g. where a member of Diocesan personnel identifies that Personal Data has been sent to the wrong email address;

5.1.2 being reported to the Diocese by a Data Subject: e.g. where a Data Subject notifies us that they have received Personal Data relating to another Data Subject;

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

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

5.2 Examples of an incident are as follows, but not limited to:

5.2.1 the disclosure of confidential data to unauthorised individuals;

5.2.2 the loss or theft of records;

5.2.3 the loss or theft of devices or equipment that may contain Personal Data;

5.2.4 a suspected breach of IT security that could have allowed unauthorised access to Personal Data;

5.2.5 a breach of physical security e.g. forcing of a door or window to gain access to a secure room;

5.2.6 the alteration of records without the authorisation of the Data Subject.

6. REPORTING AN INCIDENT

6.1 Whenever an incident is identified, the person who has identified the incident must contact the DPL immediately, preferably by telephone. This person will then be required to complete a Data Breach Incident Notification form which must be sent to the Diocese as soon as possible. The form can be requested on 0191 2433317, at data.protection@diocesehn.org.uk or it can be found on the Diocesan website at www.rcdhn.org.uk/dataprotection/dataprotection.php

7. REMEDIAL ACTION

7.1 Following the reporting of the issue, the DPL shall advise the relevant members of Diocesan personnel what remedial action must be taken.

7.2 Remedial action should seek to mitigate any risks the individual has been exposed to as a result of the breach and to prevent similar breaches occurring in the future. Action will be dependent on case specifics. If there is any doubt at all about the remedial action required to be taken, the DPL will contact the Diocese's legal advisors.

8. RISK ASSESSMENT

8.1 Using the information provided in the Data Breach Incident Notification Form and with the assistance of the reporting individual, the DPL will complete the Data Breach Assessment Form and log the incident.

8.2 The DPL will make an initial assessment of whether the incident is classed as a Personal Data breach.

8.3 If the incident is not classed as a Personal Data breach, no further actions will be required.

8.4 If the incident is classed as a Personal Data breach, the DPL will assess the severity of the breach. If the breach is deemed not likely to result in a risk to the rights and freedoms of natural persons, there will be no need to notify the Information Commissioner's Office (ICO) or the Data Subjects. The incident will be logged and any further remedial action will be decided upon.

8.5 If it is deemed that the Personal Data breach could possibly result in a risk to the rights and freedoms of natural persons, the breach will be reported to the Diocesan "Data Breach Committee" (DBC) who will be responsible for assessing the breach and deciding if it needs to be reported to the ICO.

9. NOTIFYING THE INFORMATION COMMISSIONER'S OFFICE

9.1 Under the GDPR, there is an obligation to report a Personal Data breach to the ICO 'without undue delay' and in any event within 72 hours of the Diocese becoming aware of the breach.

9.2 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 DBC.

9.3 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.

9.4 The DPL will be responsible for reporting a breach to the ICO and to any other authorities.

10. NOTIFYING DATA SUBJECTS

10.1 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 DPL must inform them

of the breach. The DBC will make the final decision as to whether notifying individuals is required and what explanation is provided to them.

10.2 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.

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

11. EVALUATION AND RESPONSE

11.1 The DPL will investigate the causes of the Personal Data breach, analysing how the breach occurred and ensuring action has been taken to ensure similar breaches do not occur again.

11.2 Confirmation of this action will be reported and logged by the DPL.

11.3 Relevant policies and procedures will be assessed in light of the incident and if necessary, will be updated.

11.4 Where necessary, training for those involved in the breach will be undertaken.

12. RECORDING

12.1 Once the DPL has confirmed that remedial action and any appropriate follow-up action has been taken, then the breach can be marked as closed, provided:

12.1.1 the individual is satisfied with the remedial action taken in respect of the breach; and

12.1.2 the DPL is satisfied that regulatory procedures have been followed.

12.2 A copy of all breach forms will be kept by the DPL and stored by the Department for Finance and Operations.

13. CONTACTS

13.1 Any queries or complaints regarding Data Breaches or data protection generally, should be addressed to the Diocesan Data Protection Lead who can be contacted by email at data.protection@diocesehn.org.uk by telephone on 0191 2433317 or at the following address: Diocese of Hexham and Newcastle, St Cuthbert's House, West Road, Newcastle upon Tyne, NE15 7PY.

14. SUPERVISORY AUTHORITY

14.1 If you remain dissatisfied with our actions, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). The ICO can be contacted by post at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, by telephone on 0303 123 1113 (local rate) or 01625 545 745 (national rate), or by email at enquiries@ico.org.uk

15. COMPLIANCE

15.1 Compliance with this policy is mandatory and Diocesan personnel are responsible for knowing and understanding this policy.

15.2 Where violation of this policy is found to be through wilful disregard or negligence, diocesan personnel may be subject to a disciplinary process.

15.3 Diocesan personnel must alert the DPL if they become aware of any breach of this policy.

16. GLOSSARY

The **"Diocese"** means the Diocese of Hexham and Newcastle. The Diocese is a charity registered with the Charity Commission in England and Wales (no 1143450). The Diocese is also a registered company (no 7732977) and the registered address is St Cuthbert's House, West Road, Newcastle upon Tyne, NE15 7PY.

"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 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.

The Diocesan **"Data Breach Committee**" consists of the Chief Operating Officer, the Head of the Department for Human Resources, the Vicar General and the Data Protection Support Manager.

17. APPROVAL AND AUTHORISATION

Name	Role	Date
Author: Catherine Joyce	Data Protection Support Manager	June 2019
Approved:	Diocesan Board	13 June 2019

18. CHANGE HISTORY

Version	Date	Reason	Initials

19. APPENDIX

- Data Breach Reporting Procedure Flowchart

DATA BREACH REPORTING PROCEDURE FLOWCHART