DIOCESE OF Hexham & Newcastle

Subject Access Request 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 all Diocesan personnel.

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

3. PURPOSE

3.1 A "Subject Access Request" is a request made by, or on behalf of, a Data Subject for Personal Data held by the Diocese about that individual.

3.2 The purpose of this policy is to have a standardised approach throughout the Diocese in the event of a Subject Access Request.

3.3 The policy explains how the Diocese will meet legal requirements, in particular of Article 15(1) of the General Data Protection Regulation (GDPR), concerning specifically the right of access by Data Subjects:

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source."

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 who receive a Subject Access Request complete the necessary procedures connected with this policy.

4.3 All Diocesan personnel are responsible for their actions and for reporting any Subject Access Requests to the DPL.

4.4 All Subject Access Requests will be dealt with by the DPL.

4.5 All Diocesan personnel who receive a Subject Access Request must forward it to/inform the DPL immediately in order that such requests can be dealt with within strict deadlines set out in the Data Protection Rules.

5. MAKING A SUBJECT ACCESS REQUEST

5.1 A Subject Access Request does not have to be in a particular format. Methods of submitting a request include by email, post, verbal request and social media.

5.2 The recommended method of making a request is by using the Diocesan Subject Access Request Form. This is available by request 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. Using this form is not compulsory but it aids in providing the necessary information to allow the Diocese to respond to the request in line with timescales.

5.3 Requests must provide enough information to enable the Diocese to identify the Data Subject to comply with the request. If the information provided is not sufficient, the Diocese may need to contact the Data Subject for further information which may delay processing the request.

5.4 No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to cover administration costs or to supply additional copies of information previously provided.

5.5 Where the Diocese considers a Subject Access Request to be manifestly unfounded, excessive or repetitive, the Diocese may lawfully refuse to respond and if so, the DPL will inform the Data Subject of this in writing within one month.

5.6 If making a request on behalf of another person, it will be necessary for the person making the request to demonstrate that they are entitled to act on behalf of the Data Subject.

5.7 A Subject Access Request Procedure Flowchart is included in this document and details the full procedure following a request.

6. RECOGNISING A SUBJECT ACCESS REQUEST

6.1 A Subject Access Request will not always be sent directly to the DPL, therefore it is important for all Diocesan personnel to be able to recognise a request.

6.2 A request does not need to include the phrase 'Subject Access Request' as long as it is clear that the individual is asking for their own Personal Data/data on behalf of another Data Subject.

6.3 The request may appear to be something else when first presented, e.g. a freedom of information (FOI) request. If it in fact relates to the Data Subject's personal information, it should be treated as a Subject Access Request.

6.4 The request may be general and may not specify what data the subject would like to request access to. If there is any doubt about whether or not a request for information is a Subject Access Request, it should be referred to the DPL immediately.

7. VERIFYING IDENTITY

7.1 The Diocese will usually need to verify the identity of anyone making a Subject Access Request to ensure information is only given to those who are entitled to it.

7.2 The Diocese will usually request a copy of one form of photo identification to verify identity. Where possible, this should be submitted at the same time as the Subject Access Request.

7.3 If the Data Subject is unable to provide a form of photo identification, the Diocese will work with the individual to find other means of verifying their identity.

7.4 In some Subject Access Request cases, the Data Subject will be known to the Diocese and it will not be necessary to obtain proof of identity, e.g. in the case of a staff member making a request.

7.5 If the person making the application is not the Data Subject, proof will be required that they are authorised to act on behalf of the Data Subject, e.g. signed written confirmation from the Data Subject or evidence that the third party has the authority to manage the affairs of the Data Subject. They will also need to have their identification verified in the manner detailed above.

8. IDENTIFYING WHAT PERSONAL DATA IS HELD

8.1 The DPL will contact the relevant Diocesan personnel to identify if the required information, as indicated in the request, is held by the Diocese.

8.2 The DPL will work with Diocesan personnel to retrieve the requested Personal Data within the timescales.

8.3 The DPL will determine if there is any information which may be subject to an exemption.

8.4 The DPL will determine if consent is required to be provided from a third party.

9. RESPONDING TO THE REQUEST

9.1 The DPL will respond to a Subject Access Request within one calendar month, starting the day the request is received (or following identity verification if later). If the end date falls on a weekend or a bank holiday, the calendar month will end on the next working day.

9.2 If the request is complex, the Diocese may extend the period of response by up to two additional months. The Diocese will communicate with the Data Subject within one month of receiving the initial request to explain why the extension is necessary.

9.3 Information will be usually be provided by email in an electronic format unless requested otherwise or the nature of the data requires it is sent in hard copy. The Diocese will not provide personal information through social media channels in response to a Subject Access Request.

9.4 If a request is made on behalf of an individual and the Diocese believes the individual may not understand what information would be disclosed to the third party, the response may be sent directly to the individual. The individual may then choose to share the information with the third party upon review.

10. EXEMPTIONS

10.1 Data protection legislation contains exemptions from the disclosure of personal information. In some circumstances the Diocese therefore may have a legitimate reason for not complying with a Subject Access Request.

10.2 Examples where an exemption may apply include, but are not limited to:

10.2.1 Where data contains information relating to a third party for which consent to release the information cannot be obtained;

10.2.2 Repeat requests for similar or identical information where the data has not changed;

10.2.3 Publicly available information.

10.3 Situations in which an exemption may apply will be dealt with on an individual basis, weighing up the rights and freedoms of all parties involved. The DPL will make the decision on what information, if any, can be disclosed to the Data Subject.

10.4 The reason(s) for the decision will be clearly communicated in the response to the request.

11. CHILDREN AND YOUNG PEOPLE

11.1 Children and young people have a right of access to information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

11.2 Children and young people from 12 upwards are generally considered as being capable of understanding their rights and making decision regarding their own information.

11.3 When responding to a Subject Access Request from, or on behalf of, a child of 12 and over, if the DPL is confident that the child or young person understands their rights, then usually the response will be sent directly to the child/young person.

11.4 The parent/guardian will be able to exercise the child or young person's rights on their behalf if the child or young person consents to this, or if it is evident that this is in their best interests.

11.5 The Diocese will take into consideration the particular circumstances in each instance, including:

11.5.1 the child or young person's level of maturity and their ability to make decisions of this nature;

11.5.2 the nature of the personal data;

11.5.3 any court orders relating to parental access or responsibility that may apply;

11.5.4 any duty of confidence owed to the child or young person;

11.5.5 any consequences of allowing those with parental responsibility access to the child or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

11.5.6 any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

11.5.7 any views the child or young person has on whether their parents should have access to information about them.

12. CONTACTS

12.1 Any queries or complaints regarding Subject Access Requests 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.

13. SUPERVISORY AUTHORITY

13.1 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

14. COMPLIANCE

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

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

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

15. GLOSSARY

"**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.

"Data Protection Rules"
Any data protection legislation, domestic or otherwise (as may be in force or repealed or replaced from time to time), e.g. the Data Protection Act 2018 and the General Data Protection Regulation 2016/679.

16. APPROVAL AND AUTHORISATION

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

17. CHANGE HISTORY

Version	Date	Reason	Initials
1.1	27 August 2019	Updated guidance from Information Commissioner's Office	CJ

18. APPENDIX

- Subject Access Request Procedure Flowchart

SUBJECT ACCESS REQUEST PROCEDURE FLOWCHART