Subject Access Request Policy

Document Overview

Purpose	The purpose of this policy is to ensure employees understand the legislation surrounding making a subject access request and the process that they will need to follow. This policy applies to all staff with a contract of employment.
Confidentiality	This document is not confidential.
Document owner	Stephen Davenport, Director of Operations.
Status note	Final
Distribution	All DBF staff.
Required action	
Proposed next step	

Version History

Version	Date	Status Note
1.0	12/10/2018	Stephen Davenport
1.1	28/03/2022	Minor Amendments – Simone Smith
1.2	06/06/2025	Minor Amendments – Steve Davenport

1. Aims of this procedure

1.1. The Information Commissioners Office Subject Access Code of Practice recommends that any organisations that hold personal data should use the code to help them understand their obligations to provide subject access to that data, and to help them follow good practice when dealing with subject access requests (SARs). The good practice advice in the code will help all organisations – whether they are in the public, private or third sector. Although the practices that organisations adopt to respond to SARs are likely to differ, depending on their size and the nature of the personal data they hold, the underlying principles concerning subject access are the same in every case. The Coventry Diocesan Board of Finance will respond to Subject Access Requests through following the Code of Practice guidance.

1.2. The Code of Practice can be accessed at:

https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

2. Data Protection Policy

2.1. The Coventry Diocesan Board of Finance (CDBF) needs to keep certain personal information in a safe, responsible and secure manner to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

2.2. The organisation is committed to ensuring any personal data will be processed and stored in line with the UK GDPR and Data Protection Act 2018. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2.3. Please see the Coventry Diocesan Board of Finance Data Protection Policy for details that underpin this procedure.

3. Subject Access Requests

3.1. Under the General Data Protection Regulation 2016 ('GDPR') a person will have the right to ask an organisation to confirm whether or not it is processing any of their personal data.

3.2. Where that is the case they will have a right of access to that data, and to other supplementary information concerning their rights.

3.3. The supplementary information an organisation must provide includes the following:

3.3.1. the purposes of processing;

3.3.2. the categories of data processed;

3.3.3. the recipients or categories of recipients;

3.3.4. the retention period or criteria used to determine this period;

3.3.5. the individual's rights under the GDPR (e.g. right to rectification or erasure, to restrict processing or object to processing and lodge a complaint with the supervising authority)

3.3.6. information regarding the source of the data (if not collected by the organisation);

3.3.7. any automated decision taking undertaken.

3.4. Individuals are allowed this access so that they are aware of and can verify the lawfulness of the processing of their personal data.

3.5. Unless one of the exceptions applies (see sections 4 and 5) you must provide a copy of the personal data that you hold upon request.

3.6. Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

3.6.1. told whether any personal data is being processed;

3.6.2. given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;

3.6.3. given a copy of the personal data; and

3.6.4. given details of the source of the data (where this is available).

4. Responsibilities

4.1. Any person wishing to exercise this right should apply in writing to the Data Protection Officer, Stephen Davenport, contactable at:

7 Priory Row
Coventry
CV1 5EX
Stephen.Davenport@Coventry.Anglican.org
02476 521346

4.2. Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the one-month period required by the Act from receiving the written request.

4.3. Where a large quantity of information about an individual is requested, the GDPR permits us to ask the individual to specify the information the request relates to. The one-month deadline to respond to the request does not begin to run until we have received the further information required to enable us to deal with the request.

4.4. We will disclose all information that can be reasonably obtained unless there is a legal reason not to at the time of asking.

5. Fees

5.1. We will provide a copy of the personal data free of charge, however, we are able to charge a reasonable fee when a request is 'manifestly unfounded or excessive', particularly if it is repetitive.

5.2. We may also charge a reasonable fee to comply with requests for further copies of the same information.

5.3. The fee will be based on the administrative cost of providing the information.

6. Procedure

The Process

6.1. The following information will be required before access is granted:

6.1.1. Information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception. We will not request further information if the identity of the person making the request is obvious.

6.2. We may also require proof of identity before access is granted. The following forms of ID will be required:

6.2.1. Photo ID (i.e. Driver Licence or Passport)

6.3. If we require further information to verify their identity, then the one-month deadline does not begin to run until you have received the required information.

6.4. Before responding to a request, we may ask the requester for information we reasonably need to find the personal data covered by the request. We need not comply with the SAR until we have received it.

6.5. However, even if the relevant information is difficult to find and retrieve, it is not acceptable for us to delay responding to a request unless we reasonably require more information to help us find the data in question.

6.6. We will acknowledge the request in writing with an explanatory letter of the process. This letter may also be an explanation of a refusal to disclose if not a legitimate request.

Gathering of information by Data Protection Officer (DPO):

6.7. The DPO will decide which of the organisation's officers will be required to gather all the required information relating to the request and will meet with these people to facilitate gathering this information. (This process should avoid inadvertent and inappropriate sharing of information.)

Screening of information:

6.8. Screening of information should be carried out to check whether it is subject to any of the exemptions laid down under the Data Protection Agency, particularly whether it would compromise a third party's right to privacy or an investigation under progress (however, the latter would arguably involve delayed disclosure than withholding of all information). This will be carried by the DPO but with appropriate specialist advice. There needs to be a robust audit trail of decisions taken.

When we can Refuse to Respond to a Request:

6.9. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we are able to charge a reasonable fee for providing the information OR refuse to respond.

6.10. We can also refuse to respond to a request where one of the exemptions apply (see section 7 below for further details).

7. Exemptions:

7.1. Under the Data Protection Act 2018 an individual's rights to access their data under the GDPR do not apply to:

7.1.1. personal data which if disclosed could compromise national security;

7.1.2. information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;

7.1.3. situations where complying with a request would lead to self-incrimination of an offence;

7.1.4. data that is processed under an act of parliament or by the government in order to secure the health and safety of persons at work;

7.1.5. confidential references given by the data controller in confidence for the purposes of an individual's education, training or employment, or the provision of a service by them;

7.1.6. management information, i.e. personal data that is processed by the data controller for the purposes of management forecasting or management planning;

7.1.7. records of any negotiations with the requester, to the extent that releasing the information would prejudice those negotiations; and

7.1.8. information that is available to the public.

7.2. There are also exemptions for specific categories of data, including:

7.2.1. exemptions for reasons of freedom of expression and information – these are connected with journalism, literature and art;

7.2.2. data processed only for the purposes of research, history and statistics. We can provide additional guidance if you think this may apply; and

7.2.3. information connected with a person's health, education and social work records.

7.3. One of the main exemptions that organisations will be able to rely on is a restriction based on protecting the rights of others. You are not obliged to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information. This exemption does not apply, however, where the other individual has consented or it is reasonable to disclose the information without the consent of the other individual.

7.4. In deciding whether it is reasonable to disclose the information without the consent of the other person you need to take into account:

7.4.1. the type of information that would be disclosed;

7.4.2. any duty of confidentiality owed to the other person;

7.4.3. any steps you have taken to get the consent of the other person;

7.4.4. whether the other individual is capable of giving consent; and

7.4.5. any express refusal of the other person.

7.5. If challenged, the organisation must be prepared to defend their decision to apply an exemption to either the ICO or the court. Therefore a decision to refuse the subject access request should be taken at a senior level and the reasons documented for the decision made.

7.6. The overriding principle of protecting children and vulnerable adults must also be taken into account. Advice must be taken by the Diocesan Safeguarding Advisor in such cases.

Review and signing off by a senior officer

7.7. The Diocesan Secretary will need to check decisions made with regards to exemptions under the Data Protection Act and sign-off the information being disclosed. This will also involve checking that the audit trail is robust.

Disclosure

7.8. Personal and potentially sensitive information needs to be disclosed in an appropriately secure way together with explanations regarding data which has been withheld or is subject to delayed disclosure (unless, of course, such an explanation would compromise third party data or an investigation in progress).

7.9. The DPO will write to the individual inform them of the types of data held, advise them of any reasons for exemption and arrange an appropriate way for them to review the data being held on them.

Response

7.10. Following disclosure of the information to the individual, depending on the nature of data disclosed, there might need to be some form of organisational response ranging from appropriate clarification or correction of data held through to apology or legal defence. This should clearly be under the supervision of the Diocesan Secretary in all but the most routine of cases.