OADBY & WIGSTON BOROUGH COUNCIL

SUBJECT ACCESS REQUEST POLICY

Policy Version Number: 3.0
Policy Author: Data Protection Officer
Authorisation: Senior Leadership Team
Date of Next Review: February 2025

Contents

1.0 Introduction

1.1 Individuals have the right under the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR), subject to certain exemptions, to have access to their personal records that are held by Oadby and Wigston Borough Council (OWBC).

1.2 This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individual who the Council has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, audio recordings and CCTV images etc.

1.3 The Council has developed this policy to guide staff in dealing with Subject Access Requests that may be received. The aim of this policy is to inform staff so that they may advise service users on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt. This procedure sets out the processes to be followed to respond to a subject access request. This is based on the Information Commissioner's Office Subject Access Code of Practice: ICO Subject Access Code of Practice.

2.0 Engagement

2.1 This policy has been developed based on the knowledge and experience of the Policy, Compliance and Data Protection Officer. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3.0 Scope

3.1 This policy applies to all members of staff that are directly employed by the Council and for whom the Council has legal responsibility.

3.2 This procedure also applies to all third parties and others authorised to undertake work on behalf of the Council. The purpose of this procedure is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

4.0 Policy Purpose and Aims

4.1 What is a Subject Access Request?

4.1.1 A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by the Council. The Data Protection Legislation entitles all individuals to make requests for their own personal data to enable individuals to verify the lawfulness of how their information is being processed. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person). The request does not have to be in any particular form other than in writing, nor does it have to include the words 'subject access' or make any reference to the Data Protection Legislation .

4.1.2 A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way.

4.1.3 The applicant must be informed of how the application is being dealt, under which legislation and free of charge, except where the request is manifestly unfounded or excessive (see 12 below). Where an individual is unable to make a written request it is the Council's view that in serving the interest of service users it can be made verbally provided the details of that request are appropriately recorded.

4.1.4 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:

- told whether any personal data is being processed;
- 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;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

4.1.5 Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual.

4.2 How to recognise and action a Subject Access Request

4.2.1 In order for the Council to action a subject access request the following must be received:

- The request must be made in writing (This may be by letter, fax, email, or even social media, such as Facebook or Twitter). It is important to note that responses to SAR requests must be returned by a secure methodology, i.e. social media must NOT be used to return information requested. However where the applicant is not able to make the request in writing it can be received verbally and a record of the request appropriately recorded.
- Any fee levied. Fees can only be levied where the request is deemed manifestly unfounded or excessive.
- Proof of identity of the applicant and/or the applicant's representative, and proof of right of access to another person's personal information, by reasonable means (See Appendix One).
- Sufficient information to be able to locate the record or information requested.
- All requests must be responded to without delay and at the latest within one calendar month of receipt of the request. This time can be extended by a further 2 months where requests are complex or numerous. However if this is the case, OWBC must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

5.0 UK General Data Protection Regulation

5.1 If the request relates to, or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a FOI request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under the DPA and UK GDPR; and another for the remaining, non-personal information made under FOIA.

5.2 If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (EIR). Any requests made for non-personal information must be forwarded to the Compliance Team at foi@oadby-wigston.gov.uk.

5.3 It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA or the EIR is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA or the EIR to the world at large, this could lead to a breach of the data protection principles.

5.4 All SAR requests received must be forwarded to the Policy, Compliance and Data Protection Officer who will record them on the central register of requests. They will then be sent to the nominated officer within each Service Area and copied into the

relevant Head of Service (e.g. SAR's requesting access to personnel records must be sent to the Head of the People Team) without delay in order for it to be processed within the legal timescale.

5.5 Where the Council processes a large quantity of information about an individual the UK GDPR permits us to ask the individual to specify the information the request relates to. The UK GDPR does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

5.6 Where requests are manifestly unfounded or excessive, in particular because they are repetitive, OWBC can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond

5.6 Where OWBC refuses to respond we must explain this to the individual, informing them of their right to complain to the supervisory authority (the Information Commissioners Office) and to a judicial remedy without undue delay and at the latest within one month.

6.0 Assisting and Advising Service Users with Requests

6.1 Where an individual is verbally making a request we should:

- Explain that they should put the request in writing, detailing the information they are requesting and from which service to enable it to be located (if possible).
- Requesters do not have to explain their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.
- Ensure that all colleagues can recognise a SAR and deal with it in accordance with this procedure and forward it immediately to the Policy, Compliance and Data Protection Officer. This is very important as a request is valid even if the individual has not sent it directly to the person who normally deals with such requests.
- Advise the applicant to send the request to the Policy, Compliance and Data Protection Officer and to provide contact details.
- In order to comply with equality legislation, where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct.

- Note that responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g. braille.

7.0 Requests Made by a Third Party on Behalf of Others

7.1 A third party, e.g. solicitor, may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

7.2 If an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, OWBC may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

8.0 Requests on Behalf of Children

8.1 Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian. It is the child who has a right of access to the 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. Before responding to a SAR for information held about a child, we should consider whether the child is mature enough to understand their rights. If OWBC is confident that the child has the capacity to understand their rights and any implications of the disclosure of information, then the child's permission should be sought to action the request. The Information Commissioner has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

8.2 What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so.

8.3 When considering borderline cases, the following should be taken into account:

- Where possible, the child's level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;

- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

9.0 Requests in Respect of Crime and Taxation

9.1 Requests for personal information may be made by authorities such as the Police or the HMRC for the following purposes:

- The prevention or detection of crime;
- The capture or prosecution of offenders; and
- The assessment or collection of tax or duty.

9.2 A formal documented request signed by an authorised officer from the relevant authority is required before proceeding with the request. The request must make it clear that one of the above purposes is being undertaken and that not receiving the information would prejudice the investigation.

10.0 Court Orders

10.1 Any Court Order requiring the supply of personal information about an individual must be complied with.

11.0 Responding to Requests

11.1 A log of all requests received will be maintained which details:

- Date received
- Date response due (within one calendar month unless complex)
- Applicant's details,
- Information requested,
- Exemptions applied in respect of information not to be disclosed,

- Details of decisions to disclose information without the data subjects consent,
- Details of information to be disclosed and the format in which they were supplied,
- When and how supplied, e.g. paper copy and postal method used to send them.

11.2 Determine whether the person's request is to be treated as a routine enquiry or as a subject access request. If we would usually deal with the request in the normal course of business, e.g. confirming appointment times or details of public meetings planned then do so.

11.3 The following are likely to be treated as formal subject access requests:

- "Please send me a copy of my HR file or tenancy file."
- "I am a solicitor acting on behalf of my client and request a copy of his tenancy file. An appropriate authority is enclosed."

11.4 Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party. This must be obtained before releasing the information requested. This may be in the form of documentation as detailed at Appendix One.

11.5 Ensure adequate information has been received to facilitate locating the information requested.

11.6 Locate the required information from all sources and collate it ready for review by the Policy, Compliance and Data Protection Officer. This review is to ensure that the information is appropriate for disclosure, i.e. to ascertain whether any exemptions apply (e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed, or is information to be withheld due to on-going formal investigations).

11.7 Advice may be sought from the Head of Law and Democracy.

11.8 Where information in respect of other individuals is contained within the information requested, it should not be disclosed without the consent of that individual.

12.0 Fees

12.1 Generally the Council must provide a copy of the information free of charge. However a 'reasonable fee' may be levied when a request is manifestly unfounded or excess, particularly if it is repetitive.

12.2 The fee must be based on the administrative cost of providing the information.

13.0 Response

13.1 Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact as soon as possible.

13.2 It must be determined whether the information is likely to change between receiving the request and sending the response. Routine on-going business additions and amendments may be made to the personal information after a request is received; however, the information must not be altered as a result of receiving the request even if the record contains inaccurate or embarrassing information, as this would be an offence under the Data Protection Act 2018.

13.3 Check whether the information collated contains any information about any other individuals and if so, consider if it is possible to comply with the request without revealing information that relates to the third party. Ensure that consideration is given to what information the requestor may already have or obtain that may identify the third party.

Where it is not possible to remove third party identifiers you must consider the following:

- Has the third party consented to the disclosure?
- Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party? Consider the following when trying to determine what reasonable circumstances are:
  - Duty of confidence owed to the third party,
  - Steps taken to try and obtain consent,
  - Whether the third party is capable of giving consent, and
  - Any express refusals of consent from the third party.

13.4 A record of the decision as to what third party information is to be disclosed and why should be made.

13.5 Consider whether there is an obligation to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes,
- Negotiations with the requestor,
- Management forecasts,
- Confidential references,
- Information used in research, historical or statistical purposes; and
- Information covered by legal professional privilege.

13.6 If the information requested, is held by the organisation and exemptions apply then a decision must be made as to whether we inform the applicant that the information is held but is exempt from disclosure or whether we reply stating that no relevant information is held.

13.7 A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided.

It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions have altered.

13.8 If the information contains complex terms or codes, we must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms.

14.0 Preparing the Response

14.1 When the requested information is not held, inform the applicant in writing as soon as possible, but in any case by the due date.

14.2 A copy of the information should be supplied in a format agreed with the applicant. For example, if the request is received electronically then the response should be returned in an electronic format.

14.3 OWBC will have one calendar month to comply with the request starting from the date all the information necessary to deal with the request and any fee that is required has been received.

14.4 It is an offence under the Data Protection Legislation to fail to respond within this time limit, and individuals have the right to complain to the Information Commissioners Office or apply to a court.

Under no circumstances should original records be sent to the applicant.

15.0 Remote Access to Records

15.1 Where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

15.2 The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others. The information to be supplied must be reviewed by an appropriate manager and written authorisation and / or agreement of exemptions applied should be obtained for disclosure or non-disclosure of the information.

16.0 Implementation

16.1 This policy will be published on the Council website and all staff will be made aware of its publication through communications and team meetings. Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the council's disciplinary procedure.

17.0 Training and Awareness

17.1 Staff will be made aware of the policy (via the Intranet) and associated training will be provided to ensure compliance.

17.2 The Senior Leadership Team and line managers are responsible for ensuring that all staff are aware of the policy.

18.0 Monitoring and Auditing

18.1 Performance against the statutory time limits will be monitored by the Compliance Officer and will be reviewed on an annual basis and used to inform the development of future procedural documents.

18.2 This standard will be reviewed on a regular basis, and in accordance with the following on an as and when required basis:

- legislative changes;

- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

19.0 Policy Review

19.1 The policy and procedure will be reviewed a minimum of every three years by the Senior Leadership team in conjunction with Heads of Service, with changes made as required and the outcome published.

19.2 Where review is necessary due to legislative change, this will happen immediately.

Appendix 1: Registration and Authentication – Examples of Documentary Evidence

Please supply one from each of the following categories (copies only):

Personal identity

- Current signed passport
- Residence permit issued by Home Office to EU Nationals on sight of own country passport
- Current UK photo-card driving licence
- Current full UK driving licence (old version) – old style provisional driving licences are not acceptable
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the right to benefit
- Building industry sub-contractor's certificate issued by the Inland Revenue
- Recent Inland Revenue tax notification
- Current firearms certificate
- Birth certificate
- Adoption certificate
- Marriage certificate
- Divorce or annulment papers
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
- GV3 form issued to people who want to travel in the UK but do not have a valid travel document
- Home Office letter IS KOS EX or KOS EX2
- Police registration document
- HM Forces Identity Card

Active in the Community

"Active in the Community" documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the name and address of the registrant.

- Record of home visit
- Confirmation from an Electoral Register search that a person of that name lives at that address
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed)
- Local authority tax bill (valid for current year)
- Current UK photo card driving licence (if not used for evidence of name)
- Current full UK driving licence (old version) (if not used for evidence of name) 15
- Bank, building society or credit union statement or passbook containing current address
- Recent original mortgage statement from a recognised lender
- Current local council rent card or tenancy agreement
- Current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit
- Court Order