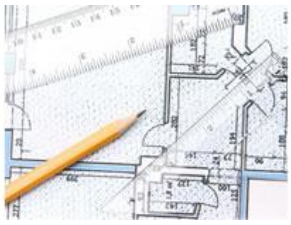
Tameside Metropolitan Borough

Subject Access Request Policy



May 2024

Document Control

Owner	Data Protection Officer
Author	Complaints and Information Requests Manager
Last Reviewer	Head of Assurance
Approver	Audit Panel
Date of Approval	June 2024
Date of Next Review	2025
Version	1.0
Classification	Public

Version Number	Date	Changes	Approved by
1.0	May 2024	Original document	Audit Panel

This is a live document effective from the issue date. It supersedes any previous version of this document, which are now withdrawn.

Further information, advice or guidance about this document can be obtained from:
The Information and Data Team
informationanddata@tameside.gov.uk

1. INTRODUCTION

1.1. Tameside Council is required under the Data Protection Act 2018 (DPA), and the General Data Protection Regulations (UK GDPR) as amended by the Data Protection Act to provide an individual with a copy of all personal information held about them following a request from the individual. This is known as the right of subject access and such a request is referred to as a Subject Access Request (SAR) or Data Subject Access Request (DSAR). The legislation noted is referred to in the policy as simply 'the legislation'.

1.2. Tameside Council will ensure that appropriate controls are implemented and maintained in relation to the processing of SARs in accordance with the requirements of the DPA to ensure that the rights of subject access to information by staff and customers can be fully exercised.

1.3. This document provides a framework for officers to meet legal and corporate requirements in relation to information requests that fall within the scope of the DPA legislation.

1.4. The Policy applies to all personal information created, received, used, and stored by Tameside Council or its contracted data processors irrespective of where or how it is held.

1.5. It must be noted that the legislation is a 'legal' requirement and the council can be fined for breaches. Individuals may also be prosecuted where data is not processed in accordance with the council's procedures.

1.6. Requests can be made verbally, however, to make the process simple and comprehensive and to help avoid any confusion or delay, requests received in writing (letter, email, online form) are preferred.

1.7. Once a request has been received, the council must give the requester access to the information they have asked for, unless an exemption applies.

1.8. Requests must be completed within a month of receiving it. If however the request is very complicated because it covers a period of many years and/or it cuts across several different services, we can take up to an additional two months. We must however advise the requester of this as soon as possible.

1.9. A detailed procedure guide on how to process and respond to a Subject Access Request can be accessed on the Information Governance Intranet page.

2. AIM OF THE POLICY

2.1. This document aims to clarify Tameside Council's legal obligations and requirements for the processing of SARs by

- defining the framework for processing SARs;
- ensuring that all requests are processed according to the current guidelines.

2.2. Tameside Council actively seeks to meet its obligations and duties in accordance with the legislation and in so doing will not infringe on the rights of its employees, customers, third parties or others.

3. SCOPE

3.1. This policy applies to all members, employees, apprentices, volunteers, contractors and third parties handling Council information. It is the responsibility of all to ensure compliance and adherence to this policy, the legislation that underpins it, and the supporting procedures and guidance.

3.2. The policy applies to any request from any living individual to access their personal information held by any part of Tameside Council. It does not apply to access to information about deceased individuals.

3.3. This policy does not apply to any request that is not made by, or on behalf of, the data subject. This type of request, which includes sharing data between organisations, is dealt with under locally agreed procedures and/or Information Sharing Protocols.

3.4. This policy does not apply to information held by schools. To access school records individuals should be asked to contact the school last attended.

3.5. This policy must be read in conjunction with the Subject Access Request Guidance document and the Redaction Guidance document

4. RELATED LEGISLATION

4.1. The following legislation is key to this policy. Please note this is **not** an exhaustive list.

Data Protection Act 2018 (DPA 2018)

4.2. The DPA 2018 governs how information about living individuals ('Personal Data') should be treated. It also gives rights to data subjects whose data is held. The Act applies to all personal data collected at any time whether held on computer or in/as a manual record, with some exemptions. The Act is enforced by the Information Commissioner's Office.

The UK General Data Protection Regulations (UK GDPR)

4.3. The GDPR as modified by the Data Protection Act 2018 and incorporated as UK GDPR, provides safeguards to individuals over the processing of their personal information and setting requirements for organisations to ensure appropriate technical and organisational measures are in place to comply with the principles of data protection. Much of the provisions relating to individual data subjects rights must be read in conjunction with the DPA 2018.

Freedom of Information Act 2000 (FOIA 2000)

4.4. This Act extended some of the provisions of the Data Protection Act to enable an applicant to access unstructured information held by/on behalf of public authorities and those bodies carrying out a public function. It also made it a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of information when a request has been made. The FOIA does not apply to personal data and cannot be used to request access to personal data.

The Adoption and Children Act 2002 (ACA 2002)

4.5. This Act restates and amends the law relating to adoption, and access to information which would enable an individual to obtain a certified copy of their birth records.

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 (FOIDP Regs 2004)

4.6. These regulations allow an authority to refuse a request, or part of a request, if to respond to it would exceed an 'appropriate limit'.

5. INDIVIDUAL'S RIGHT TO ACCESS INFORMATION

5.1. This right to access personal information is a basic principle of the legislation. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes an access request is entitled to a copy of their personal data, or a summary of the data where the original data would need to be redacted so heavily to protect other individuals' rights, and the following additional information:

- The Council's purposes for processing;
- The categories of personal data the Council is processing;
- The recipients or categories of recipient the Council has or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- The Council's retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- Confirmation of the individual's right to request rectification, erasure or restriction or to object to processing (subject to any amendments to those rights set out in Schedule 1 of the DPA 2018;
- Confirmation of the individual's right to lodge a complaint with the Information Commissioner's Office (ICO);
- Information about the source of the data, if the Council did not obtain it directly from the individual;
- Confirmation as to whether or not the Council uses automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- Details of the safeguards the Council has provided where personal data has or will be transferred to a third country or international organisation.

5.2. Further information on Subject Access Requests can be found on the Information Commissioner's Office website.

5.3. The council cannot charge a fee for SARs unless they are clearly excessive, repetitive or manifestly unfounded. In the event the council wishes to charge, the Data Protection Officer's opinion should be sought.

6. WHO CAN MAKE A SUBJECT ACCESS REQUEST?

6.1. Every individual has the right of access to personal information held about them. This includes individuals about whom a file is held (for example, service users) or any other individual who is referred to directly in that file.

6.2. An individual is not usually entitled to know what is recorded about another individual without their consent.

6.3. A third party may act on behalf of the data subject in the circumstances below. The following types of third-party requests are common:

- An adult acting on behalf of a child, for example, a parent or carer with parental responsibility
- An adult acting on behalf of an adult without capacity, for example, carer or advocate
- An adult acting on behalf of another adult who has the capacity and has provided consent, for example, a solicitor or carer

6.4. In some circumstances a combination of types may occur, for example, a solicitor acting on behalf of a parent acting on behalf of a child.

6.5. Other types of third-party requests, which are not made on behalf of the data subject, are dealt with under the Data Protection Policy and in the sections below. This includes data sharing between organisations and requests from the police.

7. DECIDING IF IT IS A SUBJECT ACCESS REQUEST

7.1. Council officers will need to determine whether a person's request will be treated as a routine enquiry or as a subject access request. Any written or verbal enquiry that asks for information you hold about the person making the request can be construed as a subject access request, but in many cases, there will be no need to treat it as such.

7.2. If the request is usually dealt with within the normal course of business, then the response should be treated as such. Examples of such requests might be:

- "Please send me a copy of my council tax bill"
- "How many payments did I make into my account last month?"

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

- "Please send me a copy of my staff records."
- "I have a right to see all the invoices issued to me for the last 3 years. Please send copies to me."
- "I am a solicitor acting on behalf of my client and request a copy of his social care records. An appropriate authority is enclosed."

7.4. If there is any doubt about how to respond, go back to the individual or their representative and clarify the situation.

8. COMPLAINTS ABOUT SUBJECT ACCESS REQUESTS

8.1. Where a requester is not satisfied with the response to their SAR, the Council offers an internal review. Where a complaint is received directly by the service the Information Requests Team must be notified as a matter of urgency so that the appropriate course of action can be determined.

8.2. In addition to the internal review process, a data subject may also refer their complaint to the ICO or may take action through the courts to enforce their right of subject access.

9. ROLES AND RESPONSIBILITIES

9.1. All SAR requests should be sent directly to the Information Requests Team (Executive Support), who log and acknowledge the request and will if required, conduct identification checks and seek clarification of the SAR. They will then hand over the SAR to the appropriate officer within the relevant Directorate to review and respond. Where a request is received by a service area directly, they will be responsible for ensuring that the request is logged within 24 hours of receiving it by sending a copy of the request by email to Information Request Team: informationanddata@tameside.gov.uk

Employees

9.2. All employees are responsible for recognising a SAR and following the appropriate steps to progress it, whether this means gathering the information requested personally, or transferring it to the appropriate person to deal with.

Managers

9.3. All managers are responsible for being aware of the SAR procedure and ensuring compliance by their team members. They are also responsible (where nominated by the Head of Service) for approving the response, notifying the Directorate Information Governance (IG) Champions of issues, and seeking advice and assistance where needed.

Heads of Service

9.4. Heads of Service are assigned responsibility for the main systems and information assets within their business area. The Head of Service is responsible for monitoring compliance with the DPA 2018/UK GDPR with respect to the information they 'own', which includes compliance with the right of subject access. They are responsible for selecting appropriate employees within their Service to be responsible for dealing with SARs and identifying different senior employees within their Service to act as Directorate IG Champions.

10. THIRD PARTY REQUESTS

10.1. Where Tameside Council receives a request from a third party (for example, a family member or a representative/solicitor acting for a data subject), information can only be released where the data subject has given consent. The consent must be in writing with a signed authority/letter from the data subject.

10.2. If a request is made by a third party over the phone, where the data subject is not present, officers should advise the third party to put the request in writing and send it to the Information Requests Team informationanddata@tameside.gov.uk on their headed paper (if the request is from a public/private organisation), with signed consent from the third party, clearly stating what information is required and the purpose for which it is required.

10.3. Tameside Council can then properly consider the request by providing only the information that is necessary to meet the request

11. HEALTH, SAFETY AND WELFARE OF DATA SUBJECTS

11.1. Personal data should only be disclosed over the telephone in emergencies (for example, to the Police, Social Services, or Medical Professional), where the health,

safety, or welfare (vital interests) of the data subject would be at stake. If data has to be disclosed by telephone, it is good practice to ask the third party for their switchboard number and to call them back. If in doubt, get advice from a senior member of staff.

12. DISCLOSURE TO THE POLICE AND LAW ENFORCEMENT AGENCIES

12.1. The DPA 2018 includes exemptions which allow personal data to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the data, regardless of the purpose for which the data were originally gathered. In particular, personal data may be released if:

- failure to provide the data would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty;
- failure to provide the information would put vulnerable individuals at risk;
- the information is required for safeguarding national security.

12.2. Normally, requests for information under the crime/tax exemption will be made by the Police, but it may also involve requests from other organisations that have a law enforcement role such as the Department of Works and Pensions (DWP) Benefit Fraud Section, His Majesty's Revenue and Customs (HMRC) or the Home or Foreign Offices.

12.3. It should be noted however that the Council is under no obligation to provide information to a law enforcement agency. Before providing the information, the requesting agency must provide a sufficient explanation of why the information is necessary to the extent that not providing it may prejudice an investigation. This is to satisfy the relevant information holder that the disclosure is necessary. We need to ensure that the information is being provided to a genuine and properly authorised investigation.

12.4. If we are not satisfied that there are valid grounds for releasing the information, the legislation does not oblige us to release information, and neither does the exemption require Tameside Council to disclose all personal information. In all circumstances, key questions to ask are:

- Am I sure the person is who they say they are? (for this reason, particular care should be taken if the request is made over the telephone). If in doubt, ask for the request to be made by email or in writing on headed paper.
- Is the person asking for information to prevent or detect a crime or catch or prosecute an offender? Is there a risk to a vulnerable individual?
- If I do not release the personal information, will this significantly harm any attempt by the requestor to prevent crime or catch a suspect? (The risk must be that the investigation may very well be impeded).
- If I do decide to release personal information to the requestor, what is the minimum I should release for them to be able to do their job?

12.5. Releasing information to the Police or other agencies with a law enforcement role, is a complex area, if in doubt, seek guidance from the Information Requests Team or Information Governance Team. Further guidance can be obtained via the ICO website.

12.6. **Do not be bullied into disclosing data** if you have any doubt as to the validity of the request. Either ask the third party to submit the request in writing and/ or refer the request to the Information Requests Team.

12.7. Additionally, the exemptions permitted under Schedule 2 DPA 2018 do not apply where the data subject is the victim of an actual or suspected offence that is being investigated. If the request is in respect of the victim of an offence, to be used to pre-offence histories, victim impact statements etc. the data can only be disclosed with the consent of the data subject.

13. REQUESTS FROM THIRD PARTIES THAT SHOULD BE REFUSED

13.1. Requests from agencies, such as an estate agent, debt recovery firm, or landlord, seeking information on a person who is being pursued for debt or other actions must be refused unless the consent of the data subject has been obtained. They should be informed that personal information will only be provided under the direction of a court order. Debt in particular is a civil matter not a criminal one, and as such the exemptions for the prevention and detection of crime do not apply.

13.2. There is an exemption to the above where the provision of the data is in the public interest. For example, if the council would be liable to pay the debt if the information is not provided, there may be a public interest reason for doing so. However, this must be balanced against risk to the data subject (for example, protection from abuse for vulnerable individuals).

14. TRAINING AND AWARENESS

14.1. All Tameside Council employees have a responsibility to ensure that they (and the staff they manage) have undertaken the corporate mandatory training courses that cover Data Privacy and Information Security and have sufficient awareness of the legislation so that they can comply with the requirements. All new employees to the council will also be briefed on SARS during their induction to the organisation.

14.2. All staff undertaking the processing of SARs must ensure that they follow the policies and procedures outlined in this document.

14.3. The Council will provide additional training for all staff who process SARs.

14.4. Managers should encourage and make time for their staff to attend any further Data Privacy and Information Security training or awareness opportunities that may arise.

15. SUPPORTING POLICIES

15.1. This policy should be read in conjunction with the Information Governance Framework, and in particular the following policies and procedures:

- Data Protection Policy
- Subject Access Request Guidance
- Redaction Guidance
- Freedom of Information Policy
- Personal Data Breach Reporting