

MERTHYR TYDFIL COUNTY **BOROUGH COUNCIL**

SUBJECT ACCESS REQUEST **POLICY**

Information Governance Team



MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Data Protection Officer: Lisa Richards
Information Governance Team
Civic Centre, Castle Street, Merthyr Tydfil, CF47 8AN
01685 725000
data.protection@merthyr.gov.uk

CONTENTS

PAGE

1	Introduction	1
2	Objectives	1
3	Scope	1
4	Policy Principles	1
5	Breaches of this Policy	3
6	Legal Considerations	3
7	Implementation Responsibilities	4
8	Policy Review and Maintenance	4

1. Introduction

This policy outlines the procedures in place that must be adhered to at all times when dealing with requests for information made under the Data Protection Legislation.

It sets out the principles which underpin Merthyr Tydfil County Borough Council's (the Council) approach to allow the public access to personal information we hold on them. It also reinforces the Council's commitment and intention to promote information management following set procedures when dealing with requests for information.

2. Objective

The objective of this Policy is to provide guidance on processing of Subject Access Requests (SAR). It outlines the Council's legal obligations for processing personal information in line with the Data Protection Legislation and the Information Commissioner's Office (ICO) Codes of Practice.

This Policy is intended to detail how the Council will process personal information in order to respond to SAR's. This Policy should be read in conjunction with the Privacy Standards Policy.

3. Scope

This document outlines the procedure that must be followed by Council Personnel in relation to requests for information submitted under the Data Protection Legislation.

This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of information.

This document takes into account the key features of the Data Protection Legislation and outlines how the Council will take steps to ensure compliance with that legislation in relation to requests for information.

4. Policy Principles

All personal information held by the Council will fall within the scope of the Data Protection Legislation. The legislation applies to all personal information regardless of its age, format, origin or classification. It covers files, letters, databases, reports, photographs, emails, videos, charts, maps etc. it also covers open, closed and archived information.

The Data Protection Legislation applies to all information held by the Council, including that which is provided by others. This may include another public authority, organisations, companies, members of the public etc. All information must be considered when dealing with a request.

a) Receiving a request

There are numerous ways in which the Council can receive a request for personal information. Data Subjects are encouraged to use electronic means where possible. The main contact email address for SAR's is FOI@merthyr.gov.uk or data.protection@merthyr.gov.uk.

The Council will also receive requests for personal information in the mail. In circumstances where an applicant sends a request directly to a department for response it should be passed to the Information Governance Team as soon as possible for consideration.

All SAR's must be sent to the Data Disclosure and Records Officer for processing. In circumstances where the request has been sent to another department the members of staff must forward the request to the Data Disclosure and Records Officer for processing, even if that department holds the information requested. Once the request has been received by the Data Disclosure and Records Officer the request will be acknowledged within 7 days.

b) Recording a request

All SAR's are recorded on a corporate database located in the Information Governance Team. Each request is given a specific reference number and allocated to a department for response. Once the key information has been recorded in the database the request is ready to be forwarded to the departments for a response. The SAR database will be maintained and updated when required by the Data Disclosure and Records Officer.

c) Responding to a request

The Data Disclosure and Records Officer will acknowledge each request. It will be sent to the appropriate department for consideration. This will be done via the internal email system.

Each email will outline the details of the request, guidance on the Data Protection Legislation and the date the department's response is required. It is the responsibility of all Council Personnel responsible for the request to ensure the response is received within the limits indicated. Failure to respond within this time may lead to breaches of the Data Protection Legislation.

When the SAR is received by the department the data held must be printed on single sided paper and two identical copies of the information must be sent to the Data Disclosure and Records Officer.

If there are any concerns with the information that has been requested Council Personnel are asked to discuss this with the Data Disclosure and Records Officer accordingly.

d) Time frames

In accordance with the Data Protection Legislation the Council has one calendar month to respond to each request provided relevant identity checks are carried out as illustrated below:

January has 31 days to respond
February has 28 or 29 days to respond (depending on leap year)
March has 31 days to respond
April has 30 days to respond
May has 31 days to respond
June has 30 days to respond
July has 31 days to respond
August has 31 days to respond
September has 30 days to respond
October has 31 days to respond
November has 30 days to respond
December has 31 days to respond

e) Handling a request

All requests are stored securely in the Information Governance Team. A new folder is created for each request, which are categorised by the year the request was received. Once a request has been completed it will be archived electronically. Closed files are retained and destroyed in accordance with the Council's Records Management Policy.

f) Charging for Information

In line with the Data Protection Legislation, SAR's are processed free of charge.

5. Breaches of this Policy

Breaches of this policy may result in a breach of the Privacy Standards Policy. Breaches of this policy will be considered in accordance with the Council's disciplinary policies and procedures and may result in disciplinary action up to and including dismissal.

6. Legal Considerations

In creating this policy the Council has given due regard to the following Legislative frameworks:

The Human Rights Act 1998 – Article 8 of this Act gives a right to respect for private and family life, home and correspondence. This Policy does not intend to infringe any Article 8 rights.

The Data Protection Acts and the General Data Protection Regulations – This legislation provides a legal framework which sets out how information relating to

employees, customers, clients etc. can be collected, handled and used. This Policy aims to set out how the Council will comply with SAR's across all Council departments.

The Regulation of Investigatory Powers Act 2000 – This Act covers the extent to which the Council is able to monitor and record private communications received within our telecommunication systems. It applies to all public and private communications networks.

7. Implementation Responsibilities

The Data Disclosure and Records Officer will be responsible for implementing this policy. Council Personnel will be aware of and adhere to this policy. All Heads of Service shall be responsible for implementing this policy within their areas of responsibility.

8. Policy Review and Maintenance

This policy shall be reviewed annually and at times as dictated by operational needs and changes in the Data Protection Legislation.