IF YOU HAVE ANY QUERIES REGARDING HOW YOUR PERSONAL DATA IS USED PLEASE CONTACT US ON DATA.PROTECTION@MERTHYR.GOV.UK OR 01685 725000.

Cyngor Bwrdeistref Sirol MERTHYR TUDFUL MERTHYR TYDFIL County Borough Council

Merthyr Tydfil County Borough Council

PRIVACY NOTICE

NATIONAL FRAUD INITIATIVE

This notice has been written in accordance with the General Data Protection Regulation and relevant legislation

Information Governance Team

Lisa Richards
Data Protection Officer
Sam Bishop/Maria Litchfield
Data Disclosure and Records Officer

Civic Centre, Castle Street, Merthyr Tydfil, CF47 8AN
data.protection@merthyr.gov.uk, 01685 725000

1. IMPORTANT INFORMATION

Merthyr Tydfil County Borough Council is responsible for deciding how we hold and use personal data we collect. We are required under the data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract to provide services. We may update this notice at any time if we do, we will ensure that an updated copy of this notice is made available to you as soon as reasonably practical.

It is important that you read this privacy notice together with our Privacy Standards Policy and full privacy notice which contains more detailed information about our data processing and can be accessed on our website.

We are required by law to protect the public funds we administer. We may share information provided to us with other bodies responsible for auditing or administering public funds, to prevent and detect fraud. Merthyr Tydfil County Borough Council participates in the Cabinet Office's National Fraud Initiative, a data matching exercise to assist in the prevention and detection of fraud. We are required to provide sets of data to the Minister for the Cabinet Office for data matching.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The Cabinet Offices requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Cabinet Office for matching for each exercise, and these are set out in the Cabinet Office Guidance. For further information on the Cabinet Office's legal powers and the reasons why it matches particular information, see the National Fraud Initiative privacy notice.

2. WHO WE ARE

Merthyr Tydfil County Borough Council is the data controller therefore we are responsible for the personal data we hold. The National Fraud Initiative is designed to identify fraud within the public sector by combining data sets with the aim of highlighting any errors. In Wales the National Fraud Initiative is coordinated by Audit Wales and then nationally by the Cabinet Office, who is classed as a data controller.

Merthyr Tydfil County Borough Council has appointed a Data Protection Officer who can be contacted using the details at the top of this notice.

3. WHAT PERSONAL DATA IS USED

We may collect, use, store and transfer different kinds of personal data about you as follows:

- Personal descriptors which include your name, address, email address, telephone number, date of birth
- Identification numbers, including your national insurance number, payroll number, WCCIS number
- Credit information such as your credit history
- Financial data, such as your bank details, income including benefit entitlement
- Employment data, such as your job title, employment history, this may also include whether you serve in the armed forces
- Geospatial data, such as your MAC address or IP address

We may also use and store demographic data which provides context to your personal data, such as:

- Lifestyle data, this data will include your marital status, your characteristics, general reputation, general appearance, your financial and social status, personal opinions, special dietary requirements.
- Data that relates to your family life such as the number of people living in your household, your relationships, where your children attend school, whether your children are older and are in university or are no longer living at home,

We may also process more sensitive data such as:

- Criminal data which will include details of arrests, convictions, charges or pardons, prison data, probation data, we may also obtain information from the disclosure and barring service.
- Cultural information
- Social services data which may include whether you have a looked after child, a vulnerable adult, whether you are a foster carer or care for a member of your family, care plan data and special educational needs data etc.

There are special categories of more sensitive personal data which require a higher level of protection. We collect, store and use the following special categories of personal data about you:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs

- Trade union membership
- Genetic data
- Biometric data
- Health including physical and mental health
- Sex life or sexual orientation

We explain the different methods used to collect this data about you in section 4 of this privacy notice.

4. HOW WE USE YOUR PERSONAL DATA

The National Fraud Initiative works by organisations supplying various sets of data from different information systems, in areas such as:

- payroll
- pensions
- social housing
- housing benefit
- other state benefits
- student awards
- payments to suppliers
- NHS exemptions
- record of death

You can view the full set of data specification on the government's dedicated website.

We may share information provided to us with other bodies responsible for auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.

The data supplied is input to a secure database, designed to crossmatch data items and identify:

- potential fraud
- inappropriate activity
- erroneous payments

We will collect additional personal data during our Council business functions and the services we provide to you throughout your contact with us. For more information about how your personal data is used in other service areas please visit our privacy notice webpage.

5. LEGAL BASIS FOR PROCESSING

We will only use your personal data where the data protection legislation allows us too. These will include the provisions set out under the General Data Protection Regulations and where relevant the Data Protection Act 2018. We will use your personal data in the following circumstances:

Article 6(1)(c) which relates to a legal obligation.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014 and sections s12(4) and s33 of the Tax Collection and Management (Wales) Act 2016, which describe our functions and the responsibility for public funds of the Chief Finance Officer.

Under the Local Audit and Accountability Act, we are a mandatory participant in the National Fraud Initiative and consequently is required to provide the following data sets to the Cabinet Office as part of the data matching exercise:

- blue badge parking permit
- creditors history
- creditors standing data
- concessionary travel pass
- deferred pensions
- personal budget
- pensions payroll
- payroll
- private residential care homes

6. SHARING YOUR PERSONAL DATA

Data will be submitted to the Cabinet Office and shared with other National Fraud Initiative participants including public and private sector organisations. The Cabinet Office shares the data as necessary to prevent and detect fraud with the Auditor General for Wales.

If data submitted by one participant matches with another, Audit Wales may share summary information with each of them.

The data matches are returned to us in a series of reports. Matches are reviewed to determine if they're significant and, if so, allow further investigations to be undertaken. Returned reports include:

- individuals claiming benefits at more than one authority
- individuals who are on payroll and also claiming benefit
- individuals recorded on more than one payroll
- failed asylum seekers or those not entitled to work in the UK
- duplicate payments to suppliers

The report highlighting staff who are employed by more than one participant will also be used to demonstrate our duty of care to employees, to confirm that working hour limits contained within the Working Time Directive are not exceeded.

There may be occasions when we must share your personal data with Welsh Government for statistical and analysis reasons. Welsh Government use personal data held by us to regulate how we discharge our public functions.

We will not transfer your data to any countries outside of the European Economic Area. If we do, we will inform you as soon as possible and you can expect a similar degree of protection in respect of your personal data.

7. HOW LONG WE KEEP YOUR PERSONAL DATA

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

Data extractions prepared for submission to the National Fraud Initiative and data downloads from the Cabinet Office are held by us until the next National Fraud Initiative exercise commences. In addition, progress reports concerning the results of participation in the National Fraud Initiative are presented to our Audit Committee. Once your data is no longer required it will be securely destroyed or pseudonymised.

The Cabinet Office have their own National Fraud Initiative privacy notice and retention periods which will provide further information on how long they keep your records for these purposes.

Details of retention periods for different aspects of your personal data are available in our Records Management Policy which is available on our website (www.merthyr.gov.uk).

8. HOW WE KEEP YOUR PERSONAL DATA SECURE

We have implemented appropriate security measures to prevent your personal data from being accidentally lost, used, accessed, altered, or disclosed in an unauthorised way. We limit access to your personal data to those employees who have a business need to know. Our employees will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. You can find out more about how we keep your personal data secure by contacting our Information Security Officer on information.security@merthyr.gov.uk.

9. YOUR LEGAL RIGHTS

In certain circumstances, you have rights under data protection laws in relation to your personal data. These are outlined in the GDPR and include:

- The right to Rectification – you have the right to ask to have your information corrected.
- The right to Restrict processing may apply – you may request that we stop processing your personal data however, this may delay or prevent us delivering a service to you. We will seek to comply with your request but may be required to hold or process information to comply with our legal duties.
- The right to not be subject to Automated decision making and profiling.
- The right of Access – you have the right to ask us for copies of your personal data. To make a request, please contact the Information Governance Team.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if you make any changes to your personal data so that we can update our records.

If you want to review, verify, or correct your personal data please contact the Data Protection Officer in writing using the contact details provided at the top of this notice.

10. FURTHER DETAILS

You also have the right to make a complaint at any time to our Data Protection Officer, whose contact details are provided above, or the Information Commissioner's Office, the UK supervisory authority for data protection issues:

Address: Information Commissioner's Office (Wales), 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH
Email: wales@ico.org.uk
Tel: 0330 414 6421

If you are looking for more information on how we process your personal data including data security, data retention, individual rights please access our full privacy policy. You can also obtain information directly from Information Commissioners Office website, www.ico.org.uk.