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

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 committed to protecting your personal data and complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We are registered with the Information Commissioner's Office (ICO) under registration number Z5957136.

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.

This privacy notice provides information on how we use your personal data within the National Fraud Initiative. Merthyr Tydfil County Borough Council is required by law to protect the public funds it administers. To support this duty, we may share information you provide with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

We participate in the Cabinet Office's National Fraud Initiative (NFI), this is a mandatory data matching exercise designed to identify and investigate potential fraud, error, or other irregularities. As part of the 2024/25 NFI exercise, the scope of data sharing has been extended to include adult social care data.
Data matching involves comparing computer records held by one body against those held by another to identify inconsistencies. These comparisons typically involve personal data and are conducted securely. Where a match is found, it may indicate a discrepancy that requires further investigation. It is important to note that a match does not automatically mean fraud has occurred, further checks are always carried out before any conclusions are drawn.

We are required to provide specific data sets to the Minister for the Cabinet Office for each NFI exercise. These data sets are outlined in the Cabinet Office Guidance. For further details on the Cabinet Office's legal powers and the rationale for matching particular types of information, please refer to the National Fraud Initiative Privacy Notice.

Our participation is governed by the Code of Data Matching Practice, which sets out our data protection responsibilities and aligns with the principles of transparency and accountability under the UK GDPR.

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:

General Personal Data which includes:

- Personal descriptors such as name, address, email, telephone, date of birth, this data is used to uniquely identify individuals and match records across datasets to detect duplicate claims, benefit fraud, or identity misuse.
- Identification numbers such as national Insurance number, payroll number, WCCIS number; this data is used to verify employment, benefit entitlement, and social care records. These identifiers help ensure accurate matching and prevent duplication or fraudulent claims.
- Credit information which relates to credit history and assists in identifying financial irregularities or undeclared income that may affect eligibility for public funds or benefits.
- Financial data which includes bank details, income, benefit entitlement and is used to detect benefit fraud, verify income declarations, and identify erroneous or duplicate payments.
- Employment data such as job title, employment history, armed forces service status and helps identify individuals claiming benefits while employed, working for multiple organisations, or misrepresenting employment status.
- Geospatial data which relates to MAC address, IP addresses and are used to detect patterns of access or anomalies in system usage that may indicate fraudulent activity or unauthorised access.

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

- Lifestyle data which includes marital status, characteristics, reputation, appearance, financial/social status, opinions, dietary requirements which is used to provide context for fraud risk profiling and helps assess eligibility for certain services or benefits.

- Family life data which includes household composition, relationships, children's school/university status and is used to verify claims related to housing benefit, council tax reduction, and education-related support.

We may also process more sensitive data such as:

- Criminal data relating to arrests, convictions, charges, prison/probation data, DBS information which is used to assess risk, ensure safeguarding, and verify eligibility for roles or services that require a clean criminal record.

- Cultural information which may be used to support equality monitoring and ensure fair access to services, though not directly used for fraud detection.

- Social services data which includes looked-after child status, vulnerable adult status, foster care responsibilities, care plans, SEN data, adult social care records which helps verify claims and funding related to adult social care and children's services, which has now been included in the NFI 2024/25 exercise.

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

These are processed only where strictly necessary, such as for safeguarding, verifying eligibility for specific services, or fulfilling legal obligations. Their use is subject to enhanced protections under GDPR.

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

4. HOW YOUR PERSONAL DATA IS COLLECTED

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

- payroll
- pensions
- social housing
- social care
- 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 to. 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 related to a legal obligation and Article 6(1)(e) which related to a public task

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 and the Legislative Reform (Disclosure of Adult Social Care Data) Order 2025 enabling the use of adult social care data within the data matching.

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

In addition to the lawful bases under the UK GDPR, we may also process your data under the Recognised Legitimate Interests introduced by the Data (Use and Access) Act 2025. This includes processing for the purposes of safeguarding and responding to emergencies, where it is necessary and proportionate to do so.

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.

- The right to Complain – you have the right to complain about how your personal data is used. To make a complaint 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, correct, request erasure, object, or request that we transfer a copy of your personal data to another party, 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.

Please note, our privacy notice's do 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.

Cymraeg

Mae'r ddogfen hon hefyd ar gael yn Gymraeg.
This document is also available in Welsh.