

Merthyr Tydfil County Borough Council
PRIVACY NOTICE

EMPLOYEE PROTECTION REGISTER

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 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.

This privacy notice provides information on how we use your personal data for the administration of the Employee Protection Register (EPR).

Merthyr Tydfil County Borough Council maintains an EPR to protect the health, safety, and welfare of its employees. The EPR records individuals who are considered to pose a credible and ongoing risk to staff due to previous incidents of violence, aggression, or other concerning behaviours.

2. WHO WE ARE

Merthyr Tydfil County Borough Council is the data controller and, as such, holds overall responsibility for the personal data it collects and processes. The Council comprises various departments, details of which are available on our official website. For the purposes of this privacy notice, references to 'the Department' specifically relate to the Council's Health and Safety Team, which operates within the People Services Department. This team is responsible for processing personal data in connection with the services outlined in this notice. This notice applies to individuals who have demonstrated threatening or violent behaviour towards Council employees, including those identified as posing a risk to the physical or psychological wellbeing of staff.

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:

To support the effective management of the Employee Protection Register (EPR), the Council may process the following categories of personal data:

Identification and Contact Information

- Full name
- Address and other contact details (e.g. telephone number, email address)

Incident-Related Information

- Details of reported incidents, including:
 - Date and time of occurrence
 - Nature and severity of the behaviour (e.g. verbal abuse, physical assault, threats)
 - Outcomes or consequences of the incident

Risk Assessment and Supporting Documentation

- Internal risk assessments conducted by the Council's Health and Safety Team
- Relevant supporting evidence, such as:
 - Witness statements
 - Photographic or video evidence (where applicable)
 - Records of previous incidents

Information from External Sources

- Verified information received from third parties, including:
 - Police and law enforcement agencies
 - Courts and legal representatives
 - Other local authorities or public bodies

We may also process more sensitive data such as:

Criminal Data (where applicable) including:

- Convictions Relevant to Staff Safety
 - Criminal offences where the individual has been convicted and the offence is deemed relevant to the safety of Council staff. This includes offences such as:
 - Assault or physical violence
 - Threats to harm individuals or property
 - Criminal damage
 - Harassment or stalking
 - Sexual offences (where false accusations or actual offences are involved)
- Information from Law Enforcement and Judicial Bodies

- Verified data received from:
 - Police
 - Courts
 - Crown Prosecution Service
 This may include:
 - Arrest records (if substantiated and relevant)
 - Court outcomes or sentencing details
 - Risk assessments or warnings issued by authorities
- False Allegations Against Staff
- Documented instances where individuals have made false accusations against Council employees, such as:
 - Theft
 - Assault
 - Sexual misconduct

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:

- Health-Related Indicators (Where Applicable)
- Mental health indicators that are directly relevant to staff safety and risk management
(Note: Such data will only be processed where it is necessary and proportionate to do so, and in accordance with applicable data protection laws.)

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

We collect personal data about you through our incident reporting forms which are completed by our staff and sent to the Health and Safety Team for analysis and inclusion in the EPR if the risks posed are deemed sufficient enough.

We will input your personal data into the EPR. Your personal data is stored on the Council's secure computer servers and only authorised personnel can access it. All personnel that have access to your personal data are provided with annual data protection and information security training.

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:

- When the processing is necessary for:
 - Compliance with a legal obligation under the Health and Safety at Work Act 1974
 - Performance of a task carried out in the public interest
 - Legitimate interests in ensuring a safe working environment for staff
- If the Council is required to process Criminal Data it will only be processed where it is necessary to protect the health and safety of Council employees and is handled in accordance with data protection laws, including Article 10 of the UK GDPR, which governs the processing of criminal offence data.
- If the Council is required to process special category data, such as health data it will only be processed if there is a substantial public interest for safeguarding our staff and preventing harm (Article 9(2)(g) UK GDPR)

6. SHARING YOUR PERSONAL DATA

The Council may share your personal data where it is considered necessary to safeguard the physical or psychological wellbeing of its employees. Access to information contained within the EPR is strictly controlled and may only be granted with the explicit authorisation of the Council's Senior Information Risk Owner (SIRO). Internally, such information is accessible solely to managers who are responsible for frontline staff and where there is a demonstrable need to mitigate potential risks arising in the course of their duties.

Access to the EPR is not granted to any external organisations, and is strictly forbidden as its sole purpose is to support the protection and safety of employees of Merthyr Tydfil County Borough Council.

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. The personal data collected in accordance with the processing detailed in this notice will be retained for 12 months. After this date, the entry in the EPR will be reviewed and where appropriate removed.

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 Object – this is not an absolute right and will depend on the reason for processing your personal information.
- The right to Erasure - you may request that we erase your personal data however, this may delay or prevent us delivering a service, or continuing to deliver a service. 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 Complaint – you have the right to complain to the Data Protection Officer if you are not happy with how the Council processes your personal data. To submit a complaint please contact the Information Governance Team on the details provided at the top of this privacy notice.

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 formal complaint at any time to 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](http://www.ico.org.uk), www.ico.org.uk.



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