

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 explains how Merthyr Tydfil County Borough Council, as the contracting authority for CymruSOC, collects, uses, and protects your personal data in relation to the CymruSOC cybersecurity initiative. CymruSOC is a Welsh national Security Operations Centre (SOC) service made up of various Welsh public sector bodies, including Councils, the National Health Service and Police Forces. The Welsh Government is also an integral partner to the CymruSOC. The SOC has been established to monitor and respond to cybersecurity threats across Wales by working with the Welsh public sector bodies; SOC will share threat intelligence with partner organisations, including the National Cyber Security Centre (NCSC), to help identify and prevent cybersecurity incidents; it has been established to protect the critical infrastructure and public services in Wales from disruption caused by cyber threats, and it will assist the partner organisation in compliance with cybersecurity laws and standards.

2. WHO WE ARE

Merthyr Tydfil County Borough Council is the data controller of the personal data relating to Merthyr Tydfil residents, therefore we are responsible for the personal data we hold. The Council is made up of different departments, details of which can be found on our [website](#). For the purposes of this privacy notice, references to 'the Department' specifically relate to the Council's ICT Department, which operates within the Finance Directorate.

The Department is responsible for managing and forwarding relevant cybersecurity data to CymruSOC. This includes data from the Council's SIEM (Security Information and Event Management) system. The SIEM system collects and analyses log event data from across the Council's IT infrastructure to detect, correlate, and send alerts on potential security threats. This data is shared with the SOC to support real-time monitoring, incident response, and threat intelligence activities.

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 which is included within the Council's SIEM systems. The data is collected from various systems across the Council's IT infrastructure. Whilst it does not collect personal data directly, the SEIM system will capture indirect identifiers which are transmitted to the system logs for security events. The type of personal data captured will relate to any individual who has an account on the Council's network and communications received electronically, which may include:

- Usernames and email addresses, this will relate to Council employees and any individual who has sent electronic communications to the Council and is used in order to identify who accessed what data or system and when.
- IP addresses (Internet Protocol address), they are collected automatically by IT systems and cybersecurity tools as part of routine network and system monitoring to trace the source of activity. An IP address is assigned to every device that connects to a network and helps route traffic between devices. When a user connects to the Council's website, system, or service, their IP address is logged by our:
 - Web servers
 - Firewalls
 - Routers
 - Proxy serversThese logs are automatically generated and stored in system logs or forwarded to a SIEM system. The IP address helps identify the source of a request or activity, which is crucial for detecting suspicious behaviour or cyberattacks.
- Device Identifiers, these are unique characteristics or metadata that can distinguish one device from another. Such as a MAC address (Media Access Control) this is an identifier that is unique to each network interface card which enables the SOC to identify the device on the network.

Collecting IP addresses and device identifiers allows the SOC to trace the origin of suspicious activity so that appropriate action can be taken against the perpetrator, it will help in detect unauthorised access attempts to our IT systems, it will use data to connect events across our IT systems and enable the Department to respond quickly to cyber incidents.

- Timestamps, which are used to log when events occurred.
- Login attempts and authentication logs which are used to detect brute-force attacks or unauthorised access.
- File access and modification records which are used to monitor for data breaches or insider threats.
- System and application logs – which may contain user actions or error messages linked to individuals.

The collection of the data listed above is essential for threat detection as it will enable the Council to identifying unusual or suspicious behaviour, such as failed login attempts or access from unknown locations. It enables the council to initiate an incident response and enable the Department to investigate and respond to security breaches or attempted intrusions. It will also be used for audit and compliance matters as it will ensure we are maintaining records for regulatory compliance and internal audits. The data will enable the SOC to complete forensic analysis which will help the partner organisations understand what happened and how to prevent recurrence. Lastly the data will enable us to undertake real-time monitoring of our IT infrastructure enabling the SOC to act quickly on emerging threats.

4. HOW YOUR PERSONAL DATA IS COLLECTED

The data described in section 3 is collected from people who use our online services, contact us by email, or interact with our digital systems. The Department manages the SIEM system that collects and logs event data from firewalls, servers, endpoint devices, applications, and network infrastructure. This data is filtered and correlated to identify potential threats and is securely transmitted to the CymruSOC platform using encrypted channels. The SOC processes this data to detect and respond to cybersecurity incidents. Access to this data is strictly controlled and monitored, with audit logs maintained for accountability. The personal data is collected and transmitted to the SOC through secure and automated processes managed by the Council's ICT Department.

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 to comply with cybersecurity and data protection laws specifically:

- The Network and Information Systems (NIS) Regulations 2018 requires the Council to implement robust cyber security practices relating to incident response and detection, business continuity and planning and also to conduct regular audits and compliance checks on our systems.
- The UK GDPR which requires the Council to implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risk. This includes using encryption, implementing access controls, undergo regular testing and evaluation of security measures and protect against unauthorised access and data breaches.
- The Data Protection Act 2018 supplements the UK GDPR and reinforces the requirement for the Council to safeguard personal data, including that which is stored within an IT infrastructure. It mandates accountability and governance, including the need for risk assessments and security policies.

Article 6(1)(e) which related to a public task and includes any functions which are in the public interest or exercise official authority, specifically:

- frameworks like the NCSC guidance and the Cyber Essentials scheme which have been adopted by the Council in order to comply with information security and data protection practice standards

Article 6(1)(f) which relates to our legitimate interests (or those of a third party) provided your interests and fundamental rights do not override those interests.

6. SHARING YOUR PERSONAL DATA

Under the UK GDPR and the Data Protection Act 2018, the Council must meet strict requirements when sharing personal data. In relation to the CymruSOC the Council has appointed a data processor to deliver the service, known as Socura. Socura is a UK based cybersecurity company specialising in managed detection and response services. Socura operates the SOC on behalf of Merthyr Tydfil County Borough Council and other participating Welsh public sector organisations.

As the designated processor, Socura is responsible for:

- Receiving and analysing SIEM data from participating organisations
- Monitoring for cybersecurity threats and vulnerabilities
- Investigating and responding to incidents, and
- Sharing relevant threat intelligence with trusted partners such as the NCSC.

Socura acts strictly under the instructions of the data controllers (Merthyr Tydfil County Borough Council and other participating organisations) and is legally bound by a formal data processing agreement that includes confidentiality, security, and data handling obligations. There are many participants to the CymruSOC which include other local authorities and public sector organisations across Wales. Each participating organisation is responsible for the personal data it processes in relation to the CymruSOC Cybersecurity Initiative.

As part of service delivery, the Council and Socura will share the data with Welsh Government for statistical and analysis reasons. Welsh Government also uses 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](#) unless the cybersecurity threat requires us to. In those circumstances all aspects of the processing will be completed in accordance with the relevant provisions of the data protection and cybersecurity laws and regulations.

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. Personal data processed by CymruSOC will be retained for the following retention periods apply:

- Security logs and network metadata – these are retained for up to 2 years as they are used to support threat detection, auditing, and forensic investigations.
- Incident reports and investigation records – these are retained for up to 7 years where linked to legal, regulatory, or disciplinary proceedings.
- User access logs and authentication data – generally these are retained for up to 2 years however depending on the system criticality and risk they may be held for up to 7 years.
- Threat intelligence and related indicators – these are retained for as long as they remain relevant to ongoing cybersecurity operations.

Please note, the retention periods above will not be relevant to any data that does not contain personal data.

Once the retention dates have expired, your personal data will be securely destroyed. 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.