MERTHYR TYDFIL COUNTY BOROUGH COUNCIL

DATA PROTECTION BREACH 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

POLICY SCHEDULE

ISSUE DATE	VERSION	HISTORY OF CHANGES	APPROVAL
16/04/2018	1	Policy Drafted	

CONTENTS **PAGE**

1. Introduction

Merthyr Tydfil County Borough Council holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to Data Subjects, reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Objective

The objective of this policy is to provide guidance to Council Personnel on the appropriate methods of handling a data breach.

This policy is intended to set out the procedure to be followed to ensure a consistent and effect approach is in place for managing data breaches.

This policy should be used and read in conjunction with the Privacy Standards Policy Procedures.

3. Scope

This policy relates to all personal and special category data held by the Council. This policy applies to all Council Personnel.

4. Policy Statement

The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Data Protection Officer, is duly authorised by the Council to keep this policy up to date and to amend, delete, add or substitute relevant provisions, as necessary.

5. Policy Principles

Where possible Council Personnel must be satisfied that they are able to detect and report a data breach if one should occur.

Council Personnel will ensure that all breaches of data protection are reported to the Information Governance Team as soon as possible.

Each service area is responsible for undertaking annual audits to determine that their breach detection and reporting is considered in-line with this policy.

6. Reporting a Breach

Any individual who accesses, uses or manages the Council's information is responsible for reporting data breach incidents immediately to the Information Governance Team.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable.

The report must contain as much detail of the incident as possible, when the breach occurred (dates and times), who is reporting it, what has happened, how the breach occurred, if the data relates to people, the nature of the information, and how many individuals are involved.

All data protection breaches should be reported to the Information Governance Team at data.protection@merthyr.gov.uk, for advice regarding whether or not a breach has occurred please contact the Information Governance Team on 01685 725092.

7. Containment and Recovery

The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the Data Protection Officer to establish the severity of the breach. The Data Protection Officer will establish whether there is anything that can be done to recover any loses and limit the damage the breach could cause.

8. Investigation and Risk Assessment

An investigation will be undertaken by the Data Protection Officer immediately after the breach being discovered or reported.

The Data Protection Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

9. Notification

If the breach needs to be reported to the Information Commissioner's Office (ICO) this must be done within 72 hours of the Council becoming aware of the breach. Failure to report a breach to the Information Commissioner within 72 hours can result in a fine of up to €10 million. The Data Protection Officer and the Information Security Officer are responsible for determining whether a breach will need to be reported to the ICO.

If the breach is likely to result in high risk of adversely affecting individuals' rights and freedoms, the Data Protection Officer will inform those individuals without undue delay. This will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Council for further information or to ask questions on what has occurred.

Officers of the Information Governance Forum will consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

10. Evaluation and Response

Once the initial incident is contained, the Data Protection Officer and other supporting officers will carry out a full review of the causes of the breach; the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

11. Sanctions

The ICO is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, ruling on complaints and taking appropriate action when the law is broken. The ICO is responsible

for ensuring compliance with the Data Protection Legislation and Data Protection in practice.

There are a number of tools available to the ICO for taking action to change the behaviour of organisations that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audits. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller for breaches of the Act.
If organisations are found to be in breach of the Data Protection Legislation the ICO may issue undertakings committing an organisation to a particular course of action in order to improve its compliance.

The ICO can serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law. The ICO conduct consensual assessments (audits) to check organisations are complying.

In cases of serious breaches the ICO may issue a monetary penalty notice, requiring organisations to pay a fine of up to €20 million.

The ICO can prosecute those who commit criminal offences under the Act. This includes organisations and individuals.

12. Breaches of this policy

If a breach of this policy has been detected it must be reported to the Information Governance Team for investigation.

Failure to abide by the rules and procedures written in this policy will be classed as a breach of this policy and may also be a breach of the Data Protection Legislation.

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.

13. 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. The Council acknowledges that employees have a reasonable expectation of privacy in the workplace. This Policy does not intend to infringe your Article 8 rights.

The Data Protection Legislation – This includes the General Data Protection Regulation and the Data Protection Act. 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 data protection across 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. The Council will abide by these Regulations and will not unlawfully intercept communications.

14. Implementation Responsibilities

The Information Governance Team shall develop, maintain, and publish processes to achieve compliance with this policy.

Employees will be aware of and adhere to all other relevant policies and procedures.

All Heads of Service shall be responsible for implementing this policy within their areas of responsibility.

15. Policy Review and Maintenance

The Data Protection Breach Policy shall be reviewed annually and at times as dictated by operational needs.

16. Policy Acceptance

All staff must confirm acceptance and adherence to the Data Protection Breach Policy and must confirm that they have read and understood the contents of this policy.

PRINT FULL NAME: _____

JOB TITLE: _____

SIGNATURE: _____

DATE: _____ / _____ /_____

(This Page should be printed and returned to the Data Protection Officer located in the Information Governance Team, Legal and Governance Services, Civic Centre)