Carmarthenshire County Council Data Protection Policy

sirgar.llyw.cymru
carmarthenshire.gov.wales

Cyngor Sir Gâr
Carmarthenshire
County Council

Information Governance

Data Protection Policy

The Council's Appropriate Policy Document as required by the Data Protection Act 2018

Contents

Cyngor Sir Gâr
Carmarthenshire
County Council

1. Data Protection legislation and personal data

1.1 The Council collects and uses personal data relating to our customers, clients, employees and residents within the County in order to provide its wide range of services as an unitary authority. In doing so, the Council is committed to complying with the requirements of Data Protection legislation across all of its services. For the purposes of this Policy, this legislation is comprised of:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

1.2 Personal data is defined as any information relating to an identifiable person who can be identified directly or indirectly by referring to an 'identifier'. In practice, a wide range of identifiers or items of information will constitute personal data, including names, addresses, unique reference numbers, online identifiers and even narrative about a person.

1.3 The UK GDPR sets out clear principles in relation to the processing of personal data.

These are:

- (a) Personal data must be processed lawfully, fairly and transparently
- (b) Personal data must be collected for specified, explicit and legitimate purposes, and other uses must be compatible with these purposes
- (c) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is used
- (d) Personal information must be kept accurate and where necessary, up to date
- (e) Personal data must not be kept for longer than is actually necessary
- (f) Personal data must be processed in a secure manner, including protection against unauthorised or unlawful use of personal data and against its accidental loss, destruction or damage, using appropriate technical and organisational measures

In addition to principles (a) to (e), the UK GDPR also includes a seventh principle, requiring a controller to take responsibility for what it does with personal data and how it complies with the other principles (the 'Accountability Principle').

1.4 The Council is committed to complying with the legislation by applying these principles across all its services.

1.5 The UK GDPR also prohibits the Council from processing personal data unless we are able to identify an appropriate legal basis for that processing.

1.6 In the main, the processing of personal data carried out by the Council is carried out on the following lawful bases:

- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council; or
- To comply with our legal obligations.

2. Special category personal data and criminal offence data – UK GDPR conditions

2.1 The UK GDPR also requires us to meet additional conditions for processing special category personal data and criminal convictions & offences data (referred to collectively as criminal offence data). The UK GDPR prohibits the processing of this kind of data unless any of the conditions set out in Article 9 can be met.

2.2 The special categories are personal data about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

2.3 Criminal offence data is defined as information about criminal allegations, proceedings or convictions.

2.4 The Council processes special category data under the following articles of the UK GDPR:

- Article 9(2)(b) – for employment, social security and social protection purposes
- Article 9(2)(g) – for substantial public interest purposes
- Article 9(2)(h) – for health and social care purposes
- Article 9(2)(i) – for public health purposes
- Article 9(2)(j) – for archiving, research and statistics purposes
- Article 10 also requires that the processing of criminal offence data is carried out under the control of official authority or if it is authorised by UK law

2.4 The DPA sets out provisions which supplement the UK GDPR, in relation to matters such as the processing of special category and criminal offence data.

3. Special category personal data and criminal offence data – supplementary provisions of the DPA

3.2 The Council relies on the following conditions in Schedule 1, Part 1 of the DPA in relation to the processing special category personal data:

- Employment, social security and social protection (as defined in paragraph 1)
- Health and social care (as defined in paragraph 2)

3.3 The Council also processes special category personal data under the following conditions in Schedule 1, Part 2 of the DPA, on grounds of substantial public interest:

- Statutory and government purposes (as defined in paragraph 6)
- Equality of opportunity or treatment (as defined in paragraph 8)
- Preventing or detecting unlawful acts (as defined in paragraph 10)
- Protecting the public against dishonesty (as defined in paragraph 11)
- Preventing fraud (as defined in paragraph 14)
- Counselling, advice or support services (as defined in paragraph 17)
- Safeguarding of children/individuals at risk (as defined in paragraph 18)
- Insurance purposes (as defined in paragraph 20)
- Occupational pensions (as defined in paragraph 21)
- Elected representatives responding to requests (as defined in paragraph 23)
- Disclosure to elected representatives (as defined in paragraph 24)

3.4 Criminal offence data is processed under the following Schedule 1, Part 2 conditions, by extension:

- Employment, social security and social protection
- Statutory and government purposes

3.5 The Council also relies on the following conditions found in Schedule 1, Part 3 of the DPA to process criminal offence data:

- Vital interests (as defined in paragraph 30)
- Personal data in the public domain (as defined in paragraph 32)
- Legal claims (as defined in paragraph 33)

4. Purpose of this Policy and its scope

4.1 To apply any of the conditions referred to under section 3 of this Policy, the Council must have in place an **Appropriate Policy Document** which explains:

- How we comply with the six data protection principles set out in the UK GDPR; and
- Our policies for the retention and erasure of personal data processed under these conditions.

4.2 This purpose of this Policy is therefore to comply with these specific legal requirements in relation to the processing of special category personal data and criminal offence data by the Council. This Policy is therefore the **Appropriate Policy Document** for the Council. However, the measures and actions taken to comply with the principles apply equally to all personal data held by the Council.

4.3 This policy applies to all employees of the Council, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

4.4 It is also recommended that the principles of this policy be adopted and applied by all Elected Members and Local Education Authority schools.

5. How we comply with the principles

5.1 Principle (a) – lawfulness, fairness and transparency

- Privacy notices are in place for all services which process personal data, including special category and criminal offence data. These notices make clear that special category and criminal offence data are being processed and set out the lawful basis for processing of this personal data. They also provide a description of the types of data being processed.

- These privacy notices are published prominently on the Council website, are provided to the public when personal data is collected from them and are referred to in other communications:

  https://www.carmarthenshire.gov.wales/home/council-democracy/data-protection/privacy-notices/

- Our privacy notices are regularly reviewed each service in consultation with the Data Protection Officer and updated to ensure that they accurately document each processing activity.

5.2 Principle (b) – purpose limitation

- Our privacy notices and records of processing activities clearly set out the purposes for which the personal data is processed and identify the lawful basis for the processing. These are regularly reviewed each service in consultation with the Data Protection Officer.

- Training for Managers and Information Asset Owners specifies the need to only use personal data for specified and limited purposes and the Data Protection Officer is consulted where a new purpose is considered.

- The Council will not process personal data for purposes that are incompatible with the original purpose it was collected for.

5.3 Principle (c) – data minimisation

- Personal data is only collected for the Council's relevant purposes and we ensure that this is not excessive. The information processed is necessary for and proportionate to the Council's purposes. Where personal data is provided or obtained but is not relevant to our stated purposes, it will be erased.

- Periodic reviews of the personal data held in individual business units are undertaken and data which is no longer needed is deleted, in accordance with the Council's Retention Guidelines.

- These Retention Guidelines set out retention periods based on legal obligations and the necessity of its retention for the Council's business needs.

- Compliance with this principle will be subject to periodic Internal Audit review.

5.4 Principle (d) – accuracy

- Where appropriate, Council services have in place review mechanisms to check that personal data remains accurate and up to date.

- Where we become aware that personal data is inaccurate or out of date, taking into account the purpose for which it is being processed, the Council will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

- Individuals are informed of their right to erasure or rectification and we carefully consider any requests received to exercise this right. We keep records of such requests from individuals.

- Managers and Information Asset Owners are subject to a training programme which specifies their obligation to regularly review, update and correct personal data.

- Compliance with this principle will be subject to Internal Audit review.

5.5 Principle (e) – storage limitation

- The Council has in place a Records Management Policy which requires that detailed Retention Guidelines are in place covering all its services, including those that process special category and criminal offence data**.** These are based on legal requirements to retain personal data for specific periods as well as the identified need of each business unit.

- The Council will utilise software which will apply a retention period to personal data in our cloud storage in SharePoint, in accordance with the Retention Guidelines, and which will subsequently delete or review the personal data that has reached its retention period.

- Other systems and databases are regularly reviewed and personal data is deleted where it has passed its retention period.

5.6 Principle (f) – integrity and confidentiality (security)

Organisational measures

- The Council has in place clear policies and procedures which require that staff keep personal data secure and provide information on how to do so:

    - **Information Security Policy**
    - **Handling Personal Data Policy**
    - **Portable Device Usage Policy**
    - **Records Management Policy**

- These are regularly reviewed, actively communicated to employees and made available for reference in prominent locations on the Council's intranet site.

- The Council provides training, comprised of e-learning and other guidance, which places an emphasis on data security.

- All personal data is processed in buildings protected from public access by swipe card entry systems.

- Personal data processed in paper format is kept in lockable storage within these areas.

- Processors used by the Council are required to implement appropriate organisational measures.

Technical measures

- Data is stored in secure data centres. Controls are in place to prevent unauthorised access to buildings and only authorised personnel may

access these data centres. Any contractors permitted access are supervised.

- A perimeter firewall controls connections between the Council's internal network and the internet. It is used to restrict bi-directional communications to only what is required, to prevent unauthorised access from the internet and to prevent unauthorised outbound transfer of data.

- Where it is a requirement under the above policies to do so, personal data sent to external parties is encrypted. Only authorised solutions are used.

- Access rights to data is managed on a per user basis and permissions to data sources are granted only when there is a requirement. Access is revoked when the requirement expires.

- Two factor authentication is utilised.

- Servers and applications are kept up to date to prevent the exploitation of know vulnerabilities that could have a negative impact on the confidentiality, integrity and availability of data. There is also anti-malware software running on all endpoint devices and at the internet gateway.

- The network is penetration tested regularly to identify and subsequently remediate any vulnerabilities to ensure the protection of data.

- A multi-layered approach to security is in place to provide a resilient defence against cyber-attacks and protection for the data we hold.

- All core systems are backed up to prevent loss of data and for recovery in the event of a disaster.

- Write access from end user devices to removeable media is restricted.

5.7 The Accountability Principle

- The Council maintains and regularly reviews records of processing activities across all of its services.

- As set out in section 5.6 above, the Council has in place appropriate policies in relation to the processing of personal data.

- Data Protection Impact Assessments are carried out for processing of personal data that are likely to result in high risk to individuals' interests.

6. Retention and erasure of personal data

6.1 The Council manages its data in accordance with its **Retention Guidelines**. These are published on the Council's website and intranet site and set out how long specific records are to be kept before they are destroyed or deleted.

6.2 Where not specified, special category and criminal offence data are included within other record types.

6.3 Erasure or destruction of personal data is carried out in accordance with our **Records Management Policy**.

7. Equalities statement

7.1 Carmarthenshire County Council must comply with the Equality Act 2010, the Public Sector Equality Duty and the Specific Duties for Wales. When making decisions and delivering services, we must have due regard to:

- Eliminating discrimination, harassment, victimisation and any other conduct that is prohibited under the Act.
- Advancing equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Fostering good relations between persons who share a relevant protected characteristic and persons who do not share it.

7.2 In addition, the Welsh Language Standards require us to ensure that 'the Welsh language is treated no less favourably than the English language' and to ensure that the Language is promoted in our communities.

If you require this document in an alternative format please email **dataprotection@carmarthenshire.gov.uk**

Policy approved by the Cabinet:
Policy written by: Information Governance Manager

Cyngor Sir Gâr
Carmarthenshire
County Council