Carmarthenshire County Council

Data Protection Policy

Cyngor Sir Gâr Carmarthenshire County Council
EICH CYNGOR arleinamdani
www.sirgar.llyw.cymru
YOUR COUNCIL doitonline
www.carmarthenshire.gov.wales

Information Governance

Data Protection Policy

Contents

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. 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 General Data Protection Regulation (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 GDPR sets out six principles relating to the processing of personal data. These are:

- Personal data must be processed lawfully, fairly and transparently
- Personal data must be collected for specified, explicit and legitimate purposes, and other uses must be compatible with these purposes
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is used
- Personal information must be kept accurate and where necessary, up to date
- Personal data must not be kept for longer than is actually necessary
- 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

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

1.5 The 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

2.1 The GDPR also requires us to meet special conditions for processing special category personal data and criminal convictions data. The GDPR prohibits the processing of this kind of data unless the special conditions 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 The special conditions which allow processing of special category personal data include:

- 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 convictions data is prohibited unless it is carried out under the control of official authority or if it is authorised by UK law

2.4 The GDPR allows the United Kingdom and member states of the European Union to supplement these provisions regarding the processing of special category and criminal conviction data, and these are found in the DPA.

3. The supplementary requirements of the Data Protection Act 2018

3.1 Section 10 and Schedule 1 of the DPA set out the exceptions from the prohibitions in the GDPR relating to processing the special categories of personal data and criminal convictions data.

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

- Employment, social security and social protection - processing necessary for the purposes of performing of exercising obligations or rights of the Council or the data subject under employment law, social security law or the law relating to social protection.

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
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Preventing fraud
- Counselling, advice or support services
- Insurance purposes
- Occupational pensions
- Elected representatives responding to requests
- Disclosure to elected representatives

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

3.5 Along with other conditions in Schedule 1, Part 3 of the DPA, the Council also extends the statutory and government purposes condition found in Part 2 to process criminal convictions data.

3.6 In order to extend this condition to process criminal convictions data, the Council must meet the substantial public interest test.

3.7 The Council considers this test is met on the following grounds:

In all the circumstances of each processing activity, the public interest in the processing of the criminal conviction data substantially outweighs the public interest in preserving the privacy of the data subject.

This is clearly the case where data subjects themselves derive benefits from the processing of the data and where the processing is necessary and proportionate in order to protect the general public, including children and vulnerable adults.

The Council keeps records of all services which process criminal conviction data and in each case, we document the public interest factors relied upon to outweigh privacy issues.

4. Purpose of this Policy and its scope

4.1 To apply any of the conditions referred to under sections 3 and 4 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 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 convictions data by 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 First data protection principle – lawfulness, fairness and transparency

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

- 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 Second data protection principle – 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.

5.3 Third data protection principle – data minimisation

- Managers and Information Asset Owners are subject to a training programme which specifies their obligation to only process the personal data which is required for their specific business function.

- 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.

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

5.4 Fourth data protection principle – accuracy

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

- Individuals are informed of their right to 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 Fifth data protection principle – 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 convictions 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 automatically apply a retention period to personal data upon its creation, 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 Sixth data protection principle – 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 Information Policy & Procedure
    - Portable Device Usage Policy
    - Breach Reporting & Response 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 has in place a training programme, comprised of e-learning and classroom based sessions, 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.

- 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.

6. Retention and erasure of personal data

6.1 The Council manages its data in accordance with its published 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 conviction data are be included within other record types.

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

7. Ensuring equality of treatment

7.1 This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

If you require this document in an alternative format please contact the Information Governance & Complaints Manager on 01267 224127 or email **dataprotection@carmarthenshire.gov.uk**

Policy approved by the Executive Board on: ….., 2018
Policy review date: …..
Policy written by: John Tillman