

# Data Protection

## Handling Personal Information Policy



## 1. Introduction

**1.1** Carmarthenshire County Council collects and uses a wide range of information about individuals in order to carry out its functions. These people include our customers, clients, employees and residents of the County. The information held about them is personal data, which is a valuable asset. Its loss, theft or misuse could have serious consequences for the individual and the Council. Personal information must therefore be processed safely and properly, whether on paper, on a computer, or when using portable devices or removable media.

**1.2** The Data Protection Act 1998 defines processing as obtaining, recording, holding and making any use of personal data, including its disclosure and disposal.

**1.3** The Data Protection Act requires us to observe eight data protection principles. The seventh data protection principle sets out a specific requirement that appropriate technical and organisational measures must be taken to protect against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data.

## 2. Purpose and Scope

**2.1** This policy is designed to ensure that personal information is handled securely, in particular its storage and transfer, in order to assist in complying with the Council's legal obligations under the Data Protection Act. It functions alongside the Council's **Data Protection Policy** and **IT Security Policies**, in particular, the **Information Security, Removable Media** and **Incident Reporting & Response Policies**.

**2.2** This policy applies to all employees and elected members of the Council, including:

- temporary employees & agency workers
- volunteers
- contractors

**2.3** It is also recommended that this policy be adopted and applied by all schools.

**2.4** This policy covers the storage and transfer of personal information by electronic and other means.

**2.5** Whilst this policy is concerned with personal information, it is recommended that it should also be applied in relation to any information which can be classed as confidential.

## 3. Responsibilities

**3.1 Employees and elected members are responsible for:**

- Protecting the personal information they process by adhering in full to this policy.

**3.2 Managers are responsible for:**

- Ensuring that their employees are made aware of this policy and have understood its requirements.

- Ensuring that that the requirements of the policy are fully implemented within their sections/teams.
- Taking appropriate action when breaches of the policy occur and ensuring that losses or thefts of personal information in any format are reported to the IT Helpdesk in accordance with the **Incident Reporting & Response Policy**.

**3.3** Breaches of this policy may lead to disciplinary action being taken against the employees responsible.

**3.4** A breach of this policy by an elected member may also constitute a breach of the Members' Code of Conduct.

## **4. Personal information**

**4.1** The terms personal information and personal data are used throughout this policy and have the same meaning.

**4.2** Any personal information held by the Council which is not in the public domain should always be treated as strictly confidential.

**4.3** The Data Protection Act defines personal data as any information that relates to a living individual who can be identified from the information, or could be used with other information we hold (or is likely to be held by us) to identify the individual. The definition also includes any expression of opinion about the individual and any indication of intentions in respect of the individual.

**4.4** In practice, this is likely to include a very wide range of data, including, but not limited to:

- Names, addresses and dates of birth
- Reference numbers, such as employee or national insurance numbers
- Personal financial information such as bank details
- Descriptive or biographical information regarding an individual
- Photographs or other images

**4.5** The Data Protection Act also provides a specific definition of sensitive personal information and we must be particularly careful when dealing with this category of data. Sensitive personal information is defined as information about:

- Racial or ethnic origin
- Political Opinions
- Religious or other beliefs of a similar nature
- Trade Union Membership
- Physical or mental health or condition
- Sexual Life
- Offences (including alleged offences)
- Criminal proceedings, outcomes and sentences

**4.6** Although not formally defined as such, personal financial details should also in practice be considered sensitive.

## **5. Use of portable devices or removable media**

**5.1** Before copying personal data to portable devices or removable media in order to store, transport or transfer the information, permission must be obtained from a senior manager.

**5.2** Personal information should only be kept on portable devices or removable media when it is absolutely necessary to do so.

**5.3** Personal data should not be kept on portable devices or removable media unless it is encrypted.

**5.4** The portable devices covered by this policy include, but are not limited to:

- Laptop computers
- Blackberry phones
- Palm Pilots/PDAs

**5.5** The removable media covered by this policy include, but are not limited to:

- USB memory sticks/storage devices
- CD-Roms and DVDs

## **6. Security**

**6.1** Paper records, portable devices and removable media containing personal information must be kept securely within office premises. This will involve keeping them in locked cupboards when not in use and ensuring that keys are not accessible to unauthorised persons. Adequate building security, including intruder alarms and code/swipe card entry systems should be in use.

**6.2** Personal information should not be left on desks where anyone can have access to it.

**6.3** Personal information held on computer systems must be password protected and must never be left on a screen if the computer is unattended.

**6.4** Personal information should not be taken out of office premises unless it is absolutely necessary to do so and only with the permission of a senior manager. A record should be kept of what information is taken off site, when it has been taken, by whom and when it has been returned.

**6.5** When taking manual files, portable devices or removable media containing personal information out of office premises, they must be carried and kept securely, and never left unattended where they can be accessed by unauthorised persons, for instance, within vehicles.

**6.6** Paper records containing personal information must only be taken home with the permission of a senior manager, who is responsible for ensuring that a suitable working environment including a means of securely storing papers such as a lockable drawer or cabinet is available.

**6.7** Paper records must not be kept in the home for longer than necessary and returned to the office premises at the earliest opportunity.

**6.8** When working from home, personal information must not be processed on IT equipment that is not owned by the Council.

**6.9** Family members or any other unauthorised persons must not be allowed to access personal information which is taken home.

## **7. Transferring personal information**

**7.1** This section applies to the movement of personal information in quantity both within the Council as well as to government departments, other local authorities, external agencies and organisations.

**7.2** Personal information should not be copied or transferred within the Council if it can be accessed on a shared drive.

**7.3** Personal information should only be transferred, internally or externally, when it is absolutely necessary to do so.

**7.4** Personal data must not be transferred or shared when anonymised or statistical information could be used as an alternative. Any personal information provided should be relevant and the minimum necessary for a specified purpose.

**7.5** Personal information must not be transferred by other means where it is possible to do so by using a secure electronic method, such as the Council's internal email system, a secure website link or a secure network for external email. This is because secure electronic transfers are far safer than the physical movement of paper based information or removable media.

**7.6** Unless the data is encrypted or a secure network such as Government Connect is used, sending personal information externally by email should be avoided as its security cannot be guaranteed. All email addresses must always be carefully checked to ensure that they are correct.

**7.7** Personal data must not be transferred using removable media unless it is absolutely necessary to do so.

**7.8** Personal information which is copied to removable media for the purpose of transferring it must be encrypted.

**7.9** An assessment of the risk posed by sending personal information by internal mail, post, courier or fax must always be carried out in order to decide whether it is appropriate to use these methods. This should involve input from a senior manager and the following should always be considered:

- The nature of the information, its sensitivity, confidentiality or value.
- The damage or distress that could be caused to individuals if the information was lost or stolen.
- The effect any loss would have on the Council.

**7.10** When a quantity of personal information is transferred externally by post, it must be sent by recorded delivery to a named recipient and in a tamper proof envelope. If it is necessary because of the sensitivity of the personal information to include a protective marking (such as “private & confidential”), it should be sent in two envelopes with the marking shown on the inner one.

**7.11** Personal information sent by internal mail must always be in a sealed envelope and addressed to a named recipient. Where the information is sensitive, the envelope should be protectively marked.

**7.12** When using a courier to transport personal information, appropriate steps must be taken to ensure that they operate within acceptable security standards.

**7.13** When faxing personal information, the following steps must be taken:

- The machine to which the fax is being sent should be situated in a secure or constantly supervised area.
- The fax number must always be checked to ensure it is correct.
- A cover sheet clearly identifying the recipient and including the sender’s name and contact details must be used.
- The recipient must be contacted beforehand and made aware that a fax is being sent.
- Confirmation must be obtained from the recipient that the fax has been received safely.

**7.14** When a secure electronic method is not available and it is not deemed appropriate to transfer personal information by internal mail, post, courier or fax, it should be hand delivered to the intended recipient and a receipt obtained which records:

- A brief description of the information provided.
- The time and date it was received.
- The name, designation and contact details of the recipient.

**7.15** Records should be kept of all external information transfers.

## **8. Retention**

**8.1** When it is no longer necessary to keep personal data on portable devices or removable media, it must be deleted immediately.

**8.2** Where a portable device is used for the purpose of collecting personal information, the information must only be kept on it for as long as absolutely necessary. The information should be saved on the server at the earliest opportunity and deleted off the device.

**8.3** In all other cases, where it is decided that it is no longer necessary to retain personal information, the Council’s **Retention Guidelines** must be referred to before deleting or destroying records.

**8.4** Paper records containing personal information must be disposed of securely, by shredding or the use of the confidential waste service in accordance with the Council’s **Records Disposal Procedure**.

**8.5** Disposal of any ICT equipment must only be carried out by IT Services in accordance with the Council's **Information Security Policy**.

## **9. Ensuring equality of treatment**

**9.1** This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation, parental or marital status.

**If you have any queries or require this document in an alternative format please contact the Information & Data Protection Officer on 01267 246108 or email [dataprotection@carmarthenshire.gov.uk](mailto:dataprotection@carmarthenshire.gov.uk)**