Handling Personal Information Policy & Procedure

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

Handling Personal Information

Policy & Procedure

Contents

1. Introduction

1.1 Carmarthenshire County Council collects and uses a wide range of information about individuals in order to carry out its functions and deliver its services. These people include our customers, clients, employees and residents of the County and the information we hold about them is their personal data. If we fail to take adequate care of the personal data we deal with and it is lost, stolen, disclosed inappropriately or otherwise misused, this could have a serious impact on the individuals concerned ranging from distress to actual physical harm. Personal information is therefore a valuable asset, but also a liability if we handle it incorrectly.

1.2 This policy and procedure is therefore designed to ensure that personal information is handled securely, in particular its storage and transfer, to assist in complying with the Council's legal obligations.

2. Definition of personal information

2.1 Personal information or data is any information that relates to a living individual, who can be identified from the information, directly or indirectly.

2.2 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

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

2.4 There are also special categories of personal information and we must be particularly careful when dealing with these. The special categories are personal information regarding:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

2.5 There are also specific requirements for information relating to criminal convictions and offences.

3. Legal background

3.1 Data Protection legislation sets out rules relating to the processing of personal data. Processing is defined as collecting, recording, storing and making any use of personal data, including its disclosure and disposal.

3.2 We are required to observe six principles relating to the processing of personal data. The sixth principle sets out a specific requirement that appropriate technical or organisational measures must be used to protect against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.

3.3 The consequences of not handling personal data correctly could have serious consequences for the Council, as administrative fines of up to €20,000,000 can be imposed for serious Data Protection breaches.

4. Policy statements

4.1 Carmarthenshire County Council is committed to processing personal information in accordance with the requirements of Data Protection legislation.

4.2 The Council views the proper handling of personal data as essential in delivering our services and maintaining the confidence of the people that we deal with.

4.3 Any personal data held by the Council which is not in the public domain will always be treated as being strictly confidential.

4.4 The Council will make maximum use of secure electronic methods to store and transfer personal data.

4.5 This policy is approved by, and has the full support of, the Council.

5. Scope

5.1 This policy and procedure applies to all personal data owned by the Council.

5.2 This policy and procedure applies to all employees of the Council, including:

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

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

6. Responsibilities

6.1 Employees are responsible for:

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

6.2 Managers and Information Asset Owners are responsible for:

- Ensuring that their employees are made aware of this policy and procedure and have understood its requirements
- Ensuring that the requirements of the policy and procedure are fully implemented within their sections/teams
- Ensuring that their employees have received appropriate training on Data Protection requirements
- Taking appropriate action when breaches of the policy and procedure occur

6.3 Breaches of this policy and procedure may lead to disciplinary action being taken against the employees responsible.

7. Use of portable devices, removable media and cloud storage

7.1 Portable devices include, but are not limited to:

- Laptop computers & tablets
- Smartphones

7.2 Removable media include, but are not limited to:

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

7.3 Personal information must not be processed on removable media that are not owned by the Council.

7.4 Personal information must not be processed on portable devices that are not owned by the Council unless an appropriate, corporately supplied control is in place. If staff are in any doubt, they should contact IT for advice.

7.5 Portable devices or removable media must only be used to collect, store, transport or transfer personal information when there is a genuine need to do so and there is no alternative method available.

7.6 Before using portable devices or removable media to collect, store, transport or transfer personal information, permission must be obtained from the relevant manager or Information Asset Owner.

7.7 Personal data must never be kept on portable devices or removable media unless it is encrypted.

7.8 Portable devices or removable media containing personal information must be stored and transported securely.

8. Secure storage of personal information

8.1 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 must be in use.

8.2 Storage of personal data in paper records should be minimised where possible.

8.3 Within Council premises, personal data must not be left unattended where anyone can have access to it, such as on desks, window sills, corridors, printers and photocopying machines.

8.4 Personal information must not be processed on computer equipment that is not owned by the Council.

8.5 Personal data processed on office based computers must be password protected and should never be left visible on a screen if the computer is unattended.

8.6 Personal information processed on computers must always be stored in an appropriate location on the Council File Plan or system and never on the hard disk of the computer. This protects the data in the event of computer failure or theft.

8.7 Personal data must never be uploaded/stored in cloud storage not provided by the Council. This includes, but is not limited to:

- Personal email accounts (such as Gmail, Hotmail)
- Dropbox
- Microsoft OneDrive

8.8 When personal information is displayed on computer screens used in a public area, it must not be visible to members of the public.

9. Taking personal information out of the office

9.1 Personal information must not be taken out of office premises unless it is absolutely necessary to do so and only with the permission of the relevant manager or the Information Asset Owner.

9.2 When paper records, portable devices or removable media containing personal information are taken out of office premises, they must be kept secure, carried safely and never be left unattended where they can be accessed by unauthorised persons such as within vehicles or in areas accessible to the public.

9.3 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. A record should be kept of what information is taken off site, when it has been taken, by whom and when it is returned.

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

9.5 Family members, or any other unauthorised persons, must not be allowed access to any personal information, in any format, which is taken home.

10. Transferring personal information outside the Council

10.1. This includes sending personal data to the following:

- Government departments
- Other local authorities
- External agencies, companies and organisations
- Our customers and clients

10.2 Personal information must only be sent outside the Council where this is in accordance with the law and it is absolutely necessary to do so.

10.3 Personal data must not be provided to any external organisation when anonymised or statistical information could be used as an alternative. Any personal information we do provide should be relevant and the minimum necessary for a specified purpose.

11. Using an electronic method to transfer information

11.1 The safest and quickest way of transferring personal information outside the Council is a secure electronic method. This must always be considered as the first option and used whenever possible. Such methods could include, but are not limited to:

- Sending email using the Council's secure email system
- Sending the information via a secure email network such PSN
- Using the Council's secure storage

11.2 When using secure email, sending to groups or lists of contacts should be avoided as this introduces the risk of disclosing personal information to recipients who are not

authorised to access it. The same care has to be taken when replying to emails, as choosing the 'reply to all' option may also result in the information being sent to unintended and unauthorised recipients.

11.3 When beginning to type an email address, several similar addresses that have been used previously will often be suggested by the email software. It is essential that the correct address is chosen before the message is sent.

11.4 Clear instructions must be included as to how the recipient is to handle the information, for example, if it is not to be passed on without first contacting the sender.

11.5 When a secure electronic method is not available and the information is not special category personal data, or otherwise likely to cause damage or distress if disclosed to a third party, then it can be sent by standard email without the need for any further assessment of risk. An example would be responding to an individual's correspondence about a prominent issue already in the public domain. Care must nonetheless be taken to ensure that the information is sent to the correct email address.

11.6 All email usage is governed by the Council's **Email Usage and Monitoring Policy**.

12. Using other methods to transfer personal data

12.1 Other methods of transferring personal data include but may not be limited to:

- Royal Mail
- Courier
- Hand delivery/collection

12.2 When a secure electronic method is not available and the information is not special category personal data, then it can be sent by Royal Mail without the need for any further assessment of risk. An example would be a letter informing a person that they have been successful in their job application. We also need to routinely send letters containing personal information to our customers, for example, in connection with benefit claims. Care must nonetheless be taken to ensure that the information is correctly addressed to a named recipient.

12.3 In the absence of a secure electronic method, when the information to be sent is special category personal data, then the following must always be considered when deciding what means of transfer is appropriate:

- The precise nature of the information, its sensitivity, confidentiality or value
- What damage or distress could be caused to individuals if the information was lost or accessed by unauthorised persons
- The effect any loss would have on the Council
- The urgency of providing the information, taking into account the effect of not sending the data, or any delay in sending the data

12.4 If it is considered appropriate to send special category personal information by Royal Mail, the following steps must be taken:

- The envelope in which the information is sent must be clearly addressed to a named recipient
- The information must be sent by a traceable method

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

12.6 When it is not deemed appropriate to transfer personal information by Royal Mail, or courier and a secure electronic method is not an option, the information should be provided by hand to the recipient, or an arrangement made for the data to be collected and a record kept which includes:

- A brief description of the information provided
- When it was provided
- The name and contact details of the recipient, and if relevant, their designation

12.7 Where appropriate, paper records containing personal data should include a watermark stating “Disclosed Copy”.

13. Checking information before it is sent

13.1 When special category personal data, or personal information that is otherwise likely to cause damage or distress if disclosed to a third party, is being sent outside the Council in any format, the sender should consider having the information checked by another person before it is sent.

13.2 The person sending the information is responsible for:

- Ensuring that the email or postal address the information is being sent to is correct
- Making sure that when information is supplied in hard copy, a named recipient of the information is clearly specified
- Ensuring that no information relating to third parties has been included in error, either in a letter/email or an attached document

13.3 If it is considered necessary for another person to check the information, the other person is responsible for:

- Checking that the email or postal address the information is being sent to is correct
- When information is being supplied in hard copy, checking that a correct named recipient of the information has been specified
- Checking that no information relating to third parties has been included in error, either in a letter/email or an attached document
- Recording that they have checked the email, letter and/or attachments

14. Transferring personal information securely within the Council

14.1 Personal data must only be transferred within the Council when it is absolutely necessary to do so. Where possible and appropriate, personal data should be accessed via the Council File Plan or system.

14.2 Personal data must not be passed from one department to another when anonymised or statistical information would be sufficient. Any information transferred must be relevant and the minimum necessary for a specific purpose.

14.3 Documents containing personal data which are transferred using the Council's internal mail service must always be sent in a sealed envelope to a named recipient. Where it is necessary to send a substantial volume of paperwork, for example one or more files, a robust, tamper proof envelope must be used.

14.4 If it is deemed inappropriate for anyone other than the intended recipient to see personal information contained in a document, the envelope must be clearly marked 'Confidential - addressee only'.

15. Retention of personal information

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

15.2 Where a portable device is used for the purpose of collecting personal information, the information should only be kept on it for as long as is absolutely necessary. The information should be saved on the Council's network at the earliest opportunity and deleted off the device.

15.3 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.

15.4 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.**

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

16. Breaches of security

16.1 These would include cases where personal data is lost or stolen, either in electronic or paper format. Other examples would include emailing personal data to an unintended recipient or accidentally placing personal data on the Council's website.

16.2 All security breaches must be reported immediately to your line manager and Breach Response Team in accordance with the Council's **Breach Reporting & Response Policy.**

16.3 Failure to report, or delay in reporting, security breaches can have potentially serious consequences for data subjects, staff, other individuals and the Council.

17. Ensuring equality of treatment

17.1 This policy and procedure 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 & Data Protection Officer on 01267 224127 or email **dataprotection@carmarthenshire.gov.uk**

Policy approved by the Executive Board on: 26th March, 2018
Policy review date: March 2020
Policy written by: John Tillman