Handling Personal Data Policy

Version 3.0

carmarthenshire.gov.wales

Cyngor Sir Gâr
Carmarthenshire
County Council

Contents

Part 1

1. Introduction

1.1 Carmarthenshire County Council (the 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 data is therefore a valuable asset, but also a liability if we handle it incorrectly.

1.2 This policy is therefore designed to ensure that personal data is handled securely, in particular its storage and transfer, to assist in complying with the Council's legal obligations. It also sets out the Council's requirements for ensuring that personal data breaches are reported and responded to in a timely and effective manner.

1.3 This policy replaces the previous Handling Personal Information Policy & Procedure and the Breach Reporting & Response Policy.

2. Compliance measurement

2.1 Compliance with this policy is mandatory. Breaches of this policy by staff may lead to disciplinary action being taken against the employees responsible.

3. Sponsor

3.1 This policy is owned by the Corporate Information Governance Group.

4. Custodian

4.1 It is the responsibility of the Data Protection Officer (DPO) to ensure that this policy is reviewed and updated.

5. Policy statements

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

5.2 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.

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

5.4 The Council will make maximum use of secure electronic methods to process personal data, including its creation, storage and transfer.

5.5 This policy is approved by, and has the full support of, the Council's Executive Board.

6. Definition of personal data

6.1 The legal definition of personal data is any information that relates to natural persons (that is, living individuals, as opposed to organisations) who can be identified, or are identifiable directly from the information, or who can be indirectly identified from the information, in combination with other information. The terms personal data and information, as used within this policy have the same meaning.

6.2 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

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

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

6.4 There are also specific requirements for personal data relating to criminal convictions and offences.

7. Legal background

7.1 Data Protection legislation (comprised of the Data Protection Act 2018 and the UK General Data Protection Regulation) 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.

7.2 We are required to observe 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

7.3 This policy is principally concerned with adhering to the sixth principle, as set out above.

7.3 The 'accountability principle', which is specified in Article 5 (2) of the UK General Data Protection Regulation also requires the Council to take responsibility for what we do with personal data and how we comply with the six principles. Appropriate measures must be in place to be able to demonstrate compliance. This policy therefore forms part of the Council's compliance with this principle.

7.4 The consequences of not handling personal data correctly could have serious consequences for the Council, as significant administrative fines can be imposed for serious personal data breaches.

8. Scope

8.1 This policy applies to all personal data owned by the Council.

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

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

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

9. Information Asset Owners

9.1 The Council's **Information Security Policy** defines Information Asset Owners as Heads of Service.

10. Responsibilities

10.1 Employees are responsible for:

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

10.2 Managers and Information Asset Owners are responsible for:

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

Part 2

11. Use of portable devices and removable media

11.1 Portable devices include, but are not limited to:

- Laptops
- Tablets
- Smartphones

11.2 Removable media include, but are not limited to:

- USB memory sticks/storage devices
- SD cards
- CD-R and DVD-R

11.3 Personal data must not be processed on removable media that are not owned by the Council.

11.4 Personal data must not be processed on a personal device unless the device has been enrolled in the Council's Bring Your Own Device scheme. If staff are in doubt, they should contact IT for further support.

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

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

11.7 Personal data must never be kept on removable media unless it is encrypted.

11.8 Portable devices or removable media containing personal data must be stored and transported securely.

12. Secure storage and use of personal data

12.1 Storage and use of personal data in the form of paper should be minimised in line with the Council's policy statement on maximising the use of secure electronic methods to store and transfer personal data.

12.2 Personal data must always be stored in an appropriate location on the Council's network and never on the hard disk of the device. This protects the data in the event of cybercrime, computer failure or theft.

12.3 Personal data must not be left unattended where unauthorised persons can have access to it, such as on desks, windowsills, corridors and printers/photocopying devices.

12.4 Personal data must not be processed on computer equipment that is not owned by the Council.

12.5 Personal data should never be left visible on a computer screen when it is unattended - the device must be locked by the user.

12.6 When using applications such as Teams to screen-share, employees must ensure that any personal data that is not intended to be shared is not visible.

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

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

12.8 Personal data must never be uploaded to the Council's intranet, social media or any website unless:

- The personal data can lawfully be placed in the public domain and is intended for publication, for instance, planning applications or images of people who have consented to this
- The publication has been approved by a senior manager or Information Asset Owner

13. Working with personal data out of the office

13.1 When working from home or in a public area, where unauthorised persons are present such as family or members of the public, they must under no circumstances be allowed to have access to Council personal data in any form. This requirement includes ensuring that:

- Personal data is not visible to unauthorised persons on laptop screens
- Personal data cannot be overheard, for instance when being discussed using Teams, any other digital communication platforms, or speaking on a telephone
- Personal data contained within any paper documents is not accessible to unauthorised persons
- Council portable devices, which are provided for work purposes only, are not used by unauthorised persons such as family members
- Where there is a genuine need to take portable devices or removable media from one location to another, they are carried safely, and not left unattended and vulnerable such as within vehicles or in areas accessible to the public

13.2 Personal data in paper form must not be taken from its storage area within Council premises unless it is absolutely necessary to do so and only with the permission of the relevant manager or the Information Asset Owner.

13.3 Paper records containing personal data must only be taken to an employee's home with the permission of the manager, who is also responsible for ensuring that:

- A means of securely storing papers such as a lockable drawer or cabinet is provided
- A record is kept of what information is taken off site, when it has been taken, by whom and when it is returned

13.4 When personal data in paper form are taken out of Council premises or moved from one location to another, they must never be left unattended where they could be accessed by unauthorised persons such as within vehicles or public areas.

13.5 Paper records containing personal data must be carried safely when being taken from one location to another and never as loose pages. A suitable case, mail pouch or similar, which can be closed securely must always be used. Papers must never be carried as loose pages.

13.6 Employees must not print, scan or photocopy documents containing personal data using devices that are not owned by the Council. This includes personal devices within the home and those available for use in retail premises.

13.7 When working from home, to prevent issues relating to secure storage and disposal, staff should refrain whenever possible from:

- Making handwritten notes containing personal data
- Creating drafts on paper containing personal data

13.8 Personal data in paper form must not be kept in the home for longer than necessary and returned/taken to Council premises at the earliest opportunity, including for disposal.

13.9 Personal data in paper form must never be disposed of in the home. Disposition must be carried out in accordance with section 19 of this document and the Council's **Records Management Policy.**

14. Virtual meetings

14.1 Where a meeting requires the discussion of any personal data, participants must ensure that it is not overheard by any person who is not authorised to access the personal data.

14.2 When arranging a virtual meeting, using Teams for instance, the organiser of the meeting must take care to ensure that the correct attendees are selected, to prevent staff who are not authorised to access any personal data being discussed joining the meeting.

15. Transferring personal data outside the Council

15.1 This includes sending personal data to the following:

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

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

15.3 Personal data must not be provided to any external organisation when anonymised, pseudonymised or statistical information could be used as an alternative.

15.4 Any personal information provided must be relevant, and the minimum necessary for a specified and lawful purpose.

16. Using an electronic method to transfer information

16.1 The safest, quickest and most cost-effective way of transferring personal data outside the Council is a secure electronic method. This must always be considered as the first option and used whenever possible. Where a portal or file sharing platform is available, this must by used in preference to sending personal data by email.

16.2 The Council utilises Transport Layer Security (TLS) to protect email sent to public sector organisations. This is therefore a secure method of transferring personal data where this is required.

16.3 Guidance on which email addresses are protected by TLS is published by the Council on its Intranet, which is updated when necessary and can be accessed via the IT Security page.

16.4 TLS does not cover email sent to any private sector recipients, which includes our customers and clients. Therefore, for all such recipients, secure methods include, but are not limited to:

- Office 365 encrypted email
- Council ShareFile

16.5 Where the content is particularly sensitive, consideration should be given to password protecting documents attached to emails to protect the personal data in the event that it is sent to the incorrect recipient and also whilst it is being kept by an intended recipient. When using password protection it is important to:

- Provide the password by a separate email, or via a different method, such as a telephone call

- Ask for confirmation of receipt of the first email containing the password before sending the second email attaching a document
- Ensure that only the copy being sent is password protected and that access to the original kept on the Council's network or system is not restricted in this way

16.6 When using email, sending to groups or lists of contacts should be avoided as this introduces the risk of disclosing personal data to recipients who are not authorised to access it.

16.7 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.

16.8 When sending an email to a number of recipients, any personal email addresses must be entered into the Blind Carbon Copy or 'Bcc' field within the message rather than the 'To' field. Doing this conceals individuals' private email addresses and prevents them from being seen by the other recipients.

16.9 When beginning to type an email address, 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. **It is the sender's responsibility to check and double check that the correct address has been entered or selected before sending the email. The importance of this cannot be over-emphasised – many personal data breaches are experienced as a result of email being sent to the wrong recipient.**

16.10 Care must also be taken when forwarding email trails. The recipients of the latest message may not be authorised to see the content of earlier emails further down the trail.

16.11 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.

16.12 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. An example would be responding to an individual's correspondence about an issue already in the public domain. Care must nonetheless be taken to ensure that the message is sent to the correct email address.

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

17. Using other methods to transfer personal data

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

- Royal Mail
- Courier

- Hand delivery/collection from Council premises

17.2 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.

17.3 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

17.4 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

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

17.6 When it is not deemed appropriate to transfer personal data 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
- The date it was provided
- The name and contact details of the recipient, and if relevant, their designation

17.7 When released to individuals, documents containing personal data should include a watermark stating “Disclosed Copy”.

18. Checking information before it is sent

18.1 When special category personal data, or personal data 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.

18.2 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

18.3 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

19. Transferring personal information securely within the Council

19.1 Personal data must only be transferred within the Council when it is absolutely necessary to do so. Wherever possible and appropriate, personal data should be accessed via the Council's network.

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

19.3 The genuine need to transfer personal data in paper form within the Council is limited, given the safer, easier and faster alternatives available. However, where it is necessary to transfer paper documents containing personal data they must always be provided in a sealed envelope addressed to a named recipient. Where it is necessary to provide a substantial volume of paperwork, for example one or more files, a robust, tamper proof envelope must be used.

19.4 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'.

20. Retention of personal information

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

20.2 Where a portable device is used for the purpose of collecting personal data, 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.

20.3 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.

20.4 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 Management Policy.**

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

Part 3

21. Personal data breaches

21.1 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.

21.2 Data Protection legislation places an obligation on the Council to document all Personal Data Breaches, in effect, to maintain an internal register of such incidents.

21.3 The Council is also required report breaches which are likely to result in a risk to the *"rights and freedoms"* of individuals to the Information Commissioner's Office (ICO) and in certain cases, inform the individuals whose personal data has been affected.

21.4 The legal definition of the term breach, as used in this policy, is as follows:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

This section of the policy therefore covers incidents where the confidentiality, integrity or availability of personal data, in any format, is compromised.

21.5 Examples of breaches include, but are not limited to:

- Loss or theft of any ICT equipment such as laptops, tablet devices, smartphones, or USB drives containing personal data
- Loss or theft of paper records, such as files, individual documents or notebooks containing personal data
- Loss or theft of financial information such as bank account or payment card details
- Accidental disclosure of information such as emails or letters sent to the wrong recipients and containing personal data
- Accidental deletion of records, affecting service delivery and potentially impacting on individuals' wellbeing
- Unauthorised access to IT systems, cyber and ransomware attacks

22. Reporting breaches

22.1 Breaches are most likely to come to light as a result of:

- A complaint or communication from a member of the public or external organisation
- A report via IT helpdesk
- Staff becoming aware of an issue during the course of their duties
- A data processor informing the Council of an incident

22.2 All breaches must be reported in accordance with this policy, regardless of the nature of the incident.

22.3 In order to ensure that breaches can be acted upon they should be reported by employees to their line manager immediately. The breach must also be reported to the Breach Response Team via a central mailbox:

databreaches@carmarthenshire.gov.uk

22.4 Out of office hours, breaches must be reported via Delta Wellbeing (0300 333 2222).

22.5 The response to data security breaches will be coordinated by the Breach Response Team, comprised of the:

- Information Governance & Complaints Manager (DPO)
- Digital Security Officer
- Manager – Information Systems, Security

22.6 Depending on the nature of the breach, one or more of these officers will lead on the co-ordination of the response.

23. Procedure for responding to breaches

23.1 The response to a breach will follow the following steps:

- Containment and recovery
- Assessment of risk
- Notification of a breach (where necessary)
- Evaluation and response

23.2 Upon being made aware of a breach, the Breach Response Team will notify the relevant manager who will then begin to document the breach using the standard **Breach Report template.**

23.3 The details of the breach will also be entered on a register of personal data breaches maintained by the DPO and an unique incident number created.

23.3 Where the breach is believed to relate to financial information such as bank account details, payment cardholder's information or of a system related to the Payment Card Industry (PCI), the Breach Response Team must implement the **PCI Breach Response Plan** immediately (attached as **Appendix 1**)

23.4 The manager will be responsible for initiating an immediate investigation into the cause(s) of the breach and identifying and implementing necessary containment & recovery actions, which must be clearly documented in the Breach Report. Examples of such actions include, but are clearly not limited to:

- Attempting to locate and retrieve lost paper records
- Finding a missing item of ICT equipment
- Ensuring that a wrongly addressed email has been deleted
- Informing the Police in the event of a theft
- Changing door access codes

23.5 The manager will then undertake an assessment of the risk(s) posed by the breach and record this in the Breach Report. This assessment must take into account:

- The type of data involved, its nature, sensitivity and volume
- Whether the subject(s) could be harmed by the breach, for example, physical risk, identity theft, fraud or damage to reputation
- Who the individuals are, for example, children or other vulnerable people such as social care clients
- The number of individuals' personal data affected

23.6 The DPO should be consulted on the assessment of risk and the ICO's **self-assessment** tool and guidance can be utilised to assist with this.

23.7 Once these steps have been completed and recorded, the Breach Report will be returned to the Breach Response Team to be referred to the Senior Information Risk Owner (SIRO), or Deputy SIRO in their absence and to the Head of Service as IAO.

23.8 The SIRO or Deputy SIRO will then determine whether it is necessary to notify the ICO of the breach, taking into consideration the circumstances as documented. In the event that notification is required, the Breach Response Team will provide the ICO with all of the information required under Data Protection legislation.

23.9 Based on the assessment of risk, the Head of Service, in consultation with the manager and Breach Response Team, will then determine whether the data subject(s) affected by the breach are to be notified**.** Where this is deemed necessary, the information to be communicated to the subject, set out in Data Protection legislation, must be provided in full.

23.10 The steps set out from 20.1 to 20.8 above must be completed within a maximum of 5 working days.

23.11 Finally, in consultation with the manager, the Breach Response Team will identify and document any further recommendations and actions required. For example, if the breach was caused by systemic and ongoing problems, then actions such as the following may be necessary:

- Changes to procedures and systems
- Review of policies
- Staff training/awareness

23.12 A copy of the completed Breach Report must always be provided to the relevant Director.

23.13 The register of personal data breaches will be made available to the members of the Corporate Information Governance Group which will also consider personal data breaches as a standing agenda item.

24. Other policies or procedures

24.1 Where a personal data breach requires further escalation due the circumstances of the case, the SIRO will determine whether to proceed with a formal investigation under the Council's **Investigation Policy**.

24.2 Where the breach constitutes a complaint, a response to the complainant will be provided in accordance with the **Council's Complaints Policy**.

24.3 Where a reported breach constitutes a breach of any other Council policies, then the requirements of the relevant policy will be followed, which may include initiating disciplinary procedures.

Part 4

25. Equalities statement

25.1 All employees are required to adopt a positive, open and fair approach and ensure the Authority's **Equality and Diversity Policy** is adhered to and applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, disability, religion and belief or non-belief, age, sex, gender reassignment, gender identity and gender expression, sexual orientation, pregnancy or maternity, marital or civil partnership status.

25.2 In addition, the Welsh Language Standards ask us to 'ensure that the Welsh language is treated no less favourably than the English language' and this principle should be adopted in the application of this policy.

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

Policy approved by the Executive Board on: ……..
Policy review date: ……

Appendix 1

PCI Breach Response Plan

In response to a potential breach relating to PCI Data Security Standard (card payments), the Breach Response Team will make immediate contact with the Council's Treasury Management Officer or Head of Financial Services, who must:

- Ensure any compromised systems are isolated from the network;
- Gather, review and analyse the logs and related information from various central and local safeguards and security controls;
- Conduct appropriate forensic analysis of any compromised systems;
- Contact appropriate internal and external departments and entities as appropriate;
- Contact the Police and/or relevant card industry security personnel, making logs and forensic details available to them as required;
- Assist the Police and card industry security personnel in their investigative process including prosecutions;
- Contact the relevant card merchant and carry out the company's specific requirements, when reporting suspected or confirmed breaches of cardholder data.