MONMOUTHSHIRE COUNTY COUNCIL

DATA PROTECTION POLICY

Good records management can save

Contents

Policy Information	3
Introduction	4
Responsibilities	7
Confidentiality	9
Data recording and storage	11
Subject Access	12
Transparency	13
Information Sharing	14
Reporting of breaches	15

Updates:

Rev 1	October 2010	Add Data Sharing note & minor updates
Rev 2	September 2011	Minor revision and addition of sections for Security; inclusion of WASPI
Rev 3	November 2011	Addition of section on breach reporting and related amendments to Responsibilities section
Rev 3a	February 2011	Amendment to section on review
Rev 4	June 2015	Update following programmed review

1. Policy information	
Organisation	Monmouthshire County Council
Scope of policy	This policy relates to Monmouthshire County Council and all of its activities which involve processing personal data
Policy operational date	Original April 2012/ Revised version 10th June 2015
Policy prepared by	**Performance Monitoring Officer**
Policy review date	The Policy is to be reviewed by the Information Governance Group every three years, commencing 1st March 2015. **Note**: Amendments to this Statement of Policy are to be undertaken in consultation with: • The Council's Monitoring Officer • Head of Legal Services • Members of the Information Governance Group

**

2. Introduction

Purpose of policy	The primary purpose of this Policy is to set out the methods which Monmouthshire County Council will adopt to ensure it complies at all times with its duties under the Data Protection Act 1998. It is not a comprehensive guide to Data Protection legislation.
Brief introduction to Data Protection Act 1998	The Data Protection Act 1998 makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The Act states that anyone who processes personal information must comply with eight principles, which are described below. It also provides individuals with important rights, including the right to find out what personal information is held about them, whether on computer or paper. Further information about Data Protection maybe found at: https://ico.org.uk/for-organisations/guide-to-data-protection/
Data Protection Principles	Monmouthshire County Council will adhere to the eight Principles of Data Protection set out in the Data Protection Act 1998 and will at all times comply with its duties under that Act. When handling personal data the Council will comply with the rights of privacy and respect for personal and family life set out in Article 8 of the Human Rights Act 1998. The eight Data Protection Principles make sure that personal information is: • Fairly and lawfully processed • Processed for limited purposes • Adequate, relevant and not excessive • Accurate and up to date • Not kept for longer than is necessary • Processed in line with your rights • Secure • Not transferred to other countries without adequate protection The Council will: (a) comply with the conditions regarding the fair collection and use of personal information; (b) meet its legal obligations to specify the purposes for which personal information is used;

	(c) collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements; (d) ensure the quality, accuracy and adequacy of personal information used (e) apply checks to determine the length of time personal information is held; (f) ensure that the rights of people about whom personal information is held, are able to be fully exercised under the act. (g) take appropriate technical, organisational and security measures to safeguard personal information; (h) ensure that personal information is not disclosed deliberately or accidentally to any unauthorised person (i) ensure that personal information is not transferred abroad without suitable safeguards.
Personal data	The definition of "personal data" is legally complex and will not be fully explained in this policy. However, in broad terms, data should be considered to be "personal" if it relates to a living person who can be identified from the data. The data will also be classed as personal if it can be used with other known data to identify a living person. "Data" also has a legal definition, but can be interpreted as any information processed by the Council. "Processing" refers to any action involving data, including collecting, amending, storing, deleting and sharing. The Data Protection Act will therefore apply to any data processed by the Council which could be used to identify a living person.

Policy statement	The Council is committed to: • complying with both the law and good practice • respecting individuals' rights • being open and honest with individuals whose data is held • providing training and support for staff who handle personal data, so that they can act confidently and consistently • Maintaining an up-to-date Notification statement with the Information Commissioner
Key risks	The Council's main risks with regard to data fall into two key areas. Information about individuals falling into the wrong hands, through poor security or inappropriate disclosure of information: • Accidental loss of data • Deliberate theft of data • Lack of vigilance by staff or lack or training Individuals being harmed through data being inaccurate or insufficient: • Vulnerable people put at risk • Inappropriate action taken by the Council, such as incorrect legal action The Council seeks to minimise these risks through the use of appropriate physical and electronic data security, policies, procedures, training and guidance.

**

3. Responsibilities

Data Protection Officer	A named member of staff shall operate as the Council's Data Protection Officer. The Data Protection Officer's responsibilities include: • Reviewing Data Protection and related policies • Advising management and other staff on Data Protection issues • Ensuring that Data Protection induction and training is available • Notification (excluding schools) • Handling or overseeing subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors • Conducting research and seeking guidance where necessary to ensure that correct advice is given • Investigate any reported breaches of the Data Protection Act or data losses and decide, in consultation with appropriate senior officers, what action should be taken, in accordance with guidance from the Information Commissioner's Office.
Specific other staff	All members of staff are responsible for the security and accuracy of the data they work with. However, some officers have specific responsibilities for Data Protection matters, such as: **Security Officer** (responsible for data security in ICT systems) – note that ICT services have now been outsourced and are provided on a contractual basis.
Team/Department managers	Each team or department where personal data is handled is responsible for drawing up local operational procedures which are consistent with this policy and corporate practice (including induction and training) to ensure that good Data Protection practice is established and followed. This includes the use of information sharing protocols where there is a regular need to share personal data. The managers must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the organisation's Notification. Managers should also liaise with the Data Protection Officer in any situation where doubt exists over proper practice.

	Managers are also responsible for ensuring that staff and volunteers are appropriately trained and fully aware of their Data Protection responsibilities. Should any breaches of the Data Protection Act 1998 be identified, such as accidental or malicious loss of data, the manager responsible for the service area must report the loss to the Data Protection Officer as soon as possible.
Staff & volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. In this document, the term 'staff' includes both paid staff and volunteers. Staff and volunteers must have received a level of training appropriate to the nature of personal data handled and the context of their work before they handle personal data. Should any breaches of the Data Protection Act 1998 be identified, such as accidental or malicious loss of data, any member of staff or volunteer must report the loss to the manager responsible for the service area as soon as possible.
Enforcement	Conduct, including negligence, which breaches Data Protection legislation or guidelines may be subject to investigation under other Council policies such as, for example, the Disciplinary Policy or the Code of Conduct, and the sanctions therein. Breaches of the Data Protection Act 1998 may render the Council and individual officers liable to prosecution and legal consequences.

**

4. Confidentiality

Scope	Confidentiality applies to a much wider range of information than Data Protection. It forms a part of the standards expected of officers and Members and is reflected in both Codes of Conduct. Confidentiality is also a common law concept. Wrongly revealing confidential information relating to a citizen, client, colleague or any other living individual would be a breach of the Data Protection Act 1998, but revealing confidential information about a deceased person, a contract, another organisation or the Council itself is also a breach of confidentiality and may be punishable in law or by disciplinary proceedings. However, information which could be considered confidential remains subject to the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and may sometimes need to be released following a formal request. It is important that all such requests are processed by the Council's Freedom of Information Officer or a departmental Coordinator in line with the Council's normal procedures, to ensure that exemptions or exceptions are applied correctly.
Understanding of confidentiality	Access to confidential information will normally be on a "need to know" basis related to the roles of officers and members. Confidentiality underpins the work of some parts of the Council, such as Social Services, and is a part of the professional training for relevant officers. Social Services practices include advising the client how information will be used and shared. Similarly, schools advise new students and their parents of information use and sharing arrangements. It may be necessary in some circumstances to release information which would be considered confidential. This will normally be to satisfy a legal requirement, such as a Freedom of Information Act request where the information is not covered by an exemption, or a request for information under the exemption at Section 29 of the Data Protection Act 1998, which deals with matters of crime and taxation.

	Such information should only be released under the Council's Freedom of Information procedure or in the case of a Data Protection Act request, with the agreement of the Council's Data Protection Officer, the Customer Relations Manager or another suitably empowered senior officer.
Communication with Data Subjects	Data subjects are normally advised at the start of the relationship how their data will be used. Some departments, such as schools and Social Services, use advisory leaflets. Others rely on a fair processing notice when requesting personal data.
Communication with staff/Members	Confidentiality forms part of the professional training of many staff groups. The expected standards are also laid out in the Codes of Conduct for staff and Elected Members. The Council also undertakes to raise awareness in officers and members by various means including, but not limited to, training.
Authorisation for disclosures not directly related to the reason why data is held	These fall into two main categories: those likely to be at the instigation, or in the interests, of the Data Subject, and those which are made in the course of official investigations. For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Data Subject not even to be informed; authorisation should be made by a Chief Officer, with the knowledge of the Council's Data Protection Officer. Advice may also be sought form the Council's Monitoring Officer.

**

5. Data recording and storage	
General	The Council has developed policies and guidance for Data Recording and storage as part of its Information Management project. This will include material concerning accuracy, updating, storage, retention and archiving. The Council are implementing Sharepoint as the corporate Electronic Document Records Management System (EDRMS) to improve document management, records management and archiving practices to ensure compliance with legislation and legal requirements.
Retention periods	Retention periods for all types of documents are defined by the Council's Retention Schedule, based on legislation and good practice.

**

6. Subject access	
Responsibility	All officers are responsible for ensuring that any valid subject access request concerning information they hold are satisfactorily responded to within 40 calendar days. A request will not be considered valid until the identity of the requestor has been verified and any fee due has been paid. An officer who receives a subject access request must contact the Data Protection Officer or a local officer with a specific Data Protection responsibility, who will oversee and expedite the process as necessary.
Procedure for making request	Subject access requests must be in writing. Use of the subject access request form Subject Access Application Form - Revised 200113 should be encouraged whenever possible, though no valid request will be rejected because a form has not been used. All members of staff are responsible for passing on anything which might be a subject access request to the appropriate officer without delay. The Data Protection Officer or the Legal Services team should be consulted whenever advice is required.
Provision for verifying identity	A search for data information following a subject access request should not be commenced until the identity of the requestor has been verified. Documents which provide acceptable verification are listed on the Subject Access Request form.
Charging	A fee of £10 may be charged for processing a subject access request.
Procedure for granting access	Information will normally be provided in permanent form, i.e. by hard or electronic copy, according to how the information is held and the wishes of the requestor. A requestor may also be granted supervised access to certain documents if this can be done without revealing any other person's personal information. Care must always be taken to ensure that the personal data of any third party is not disclosed. When redaction of third party personal data destroys the sense of a document, a summary may be provided in its place.

**

7. Transparency	
Commitment	The Council is committed to ensuring that in principle Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	The main ways in which data subjects are advised of the above are: • Fair processing notices when data is collected • On the Council's website • Other examples may include letters of employment and Members' Welcome Packs
Responsibility	All staff are responsible for ensuring that whenever they collect personal data, the data subject is advised accordingly. If in doubt, advice should always be sought from the Data Protection Officer or a local person with Data Protection responsibilities.

**

8. Information Sharing

Purpose	The Council holds a large volume of personal data which has been collected for a variety of purposes. It may be the case that information collected by one Council department would be of use to another, or to a partner organisation.
Legality	Data sharing is generally legal, provided that the provisions of the Data Protection Act 1998 are satisfied. The First and Second Data Protection Principles are particularly relevant to the sharing of personal data within the Council. Monmouthshire County Council is a single entity for data protection purposes, so most data legitimately collected can be shared with other departments of the Council provided that no purpose for which it is used is incompatible with the purposes stated when the data was collected. Any sharing with a partner organisation must also follow the Data Protection Act and satisfy the Data Protection Principles. If the Data Protection Act cannot be satisfied, personal data must not be shared. If any doubt over legality exists, personal information should not be released without the agreement of the Data Protection Officer.
Procedures	Occasional data sharing can be undertaken without any formal arrangements provided that the legal requirements are satisfied. However, if regular or large-scale data sharing is envisaged, information sharing protocols (ISP's) should be set up. The Information Commissioner's Office has provided a Framework Code of Practice as guidance. The Wales Accord on Sharing Personal Information (WASPI) is used throughout the Welsh public sector and forms a framework within which ISP's should be used.

9. Reporting of breaches

General	Any loss or improper release of personal data has the potential to cause damage or distress to those individuals who are affected by it. It is the responsibility of the Council to ensure that adequate protection is in place to prevent such incidents. The Information Commissioner has powers to use a range of enforcement and deterrent actions including the imposition of Monetary Penalty Notices (fines) up to £500,000. All breaches, however small or large, must therefore be reported to line managers, and from there to the Council's Data Protection Officer, for further consideration and action. **CONCEALING OR FAILING TO REPORT A BREACH MAY BE CONSIDERED TO BE A DISCIPLINARY MATTER.**
Definition of breach	A breach will be considered to have occurred when personal data is lost, stolen or released in circumstances when it should not have been released.
Process to be followed	When any officer reports a breach to his line manager, the line manager must promptly advise the Council's Data Protection Officer by e-mail, either directly or to foi@monmouthshire.gov.uk. The e-mail should include: • The type of information involved • The number of records released • Immediate action taken to minimise or mitigate the effect on individuals involved • Initial impression of how the breach occurred • Details of how the breach is to be investigated. In consultation with the DP Officer, the service manager will establish what remedial action is required to prevent a recurrence. The DP Officer will consider the seriousness of each reported breach, in accordance with the guidelines provided by the ICO, and decide whether it should be reported to the Information Commissioner's Office. Senior management views will be sought in any case where the impact of the breach is serious enough that advising the

	ICO is being considered. The Data Protection Officer will maintain a log of all breaches and retain all relevant communications.

END