MONMOUTHSHIRE COUNTY COUNCIL

GENERAL DATA PROTECTION REGULATION POLICY

(GDPR)

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 GDPR
Policy operational date	Original April 2012/ Revised version June 2015/ revised to reflect GDPR April 2018
Policy prepared by	Annette Evans- Customer Relations Manager & Acting Data Protection Officer Rachel Trusler- Freedom of Information & Data Protection Support Officer In consultation with Tracey Harry- Head of People & Senior Information Risk Officer (SIRO) and Information Governance Group (IGG)
Recommendation	Elected Member decision for Monmouthshire County Council to adopt and implement the policy
Approved By	
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 • Single Member

Contents

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
Rev 5	April 2018	Revisited to reflect GDPR- Accountability, Principles A-F, Retention, SAR timescales, information sharing, breach notification process and complaints including new email dataprotection@monmouthshire.gov.uk

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 General Data Protection Regulation (GDPR) and Data Protection Law. It is not a comprehensive guide to Data Protection legislation.
Brief introduction to General Data Protection Regulation	The General Data Protection Regulation strengthens individual rights and unifies data protection across the EU. Within scope of the GDPR falls any "processing" (including obtaining, holding, using, disclosing etc.) of personal data relating to living individuals. The Regulation states that controllers and processors of personal data must comply with principles A-F, which are described below: The GDPR also has the added overarching principle of accountability. The GDPR provides the following rights for individuals: • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making and profiling. Further information about GDPR may be found at: www.ico.org.uk
GDPR Principles A-F	Monmouthshire County Council will adhere to the six Principles of GDPR and will at all times comply with its duties under Data Protection Laws. 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 6 GDPR Principles A-F are: "a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every

	reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
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 but not limited to: collecting, amending, storing, deleting and sharing. The GDPR will therefore apply to any data processed by the Council and its staff which could be used to identify a living person. "Special category" data is personal data which the GDPR says is more sensitive, and so needs more protection. In order for Mon CC to process special categories of personal data, a lawful basis under GDPR article 6 will be used, along with a separate condition for processing under GDPR Article 9.For full recital information please visit www.ico.org.uk. Examples of special categories of personal data now include some biometric information and genetic data.

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 • Maintaining registration with the Information Commissioner • Providing GDPR compliant documents such as: privacy notices, explicit opt-in consent options where appropriate and compliant Data Protection Impact Assessments when undertaking new projects or if there is a potential of harm to an individual • providing training and support for staff who handle personal data, so that they can act confidently and consistently
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. (List of related policies in appendix)

3. Accountability

All individuals "processing" personal data	Under GDPR all individuals who process personal data are accountable and must be compliant.
Data Protection Officer	As a public authority we have appointed a Data Protection Officer (DPO). • Our DPO reports directly to our Senior Information Risk Officer (SIRO) and Information Governance Group (IGG) and is given the required independence and resources to perform their tasks. • We involve our DPO, in a timely manner, in all issues relating to the protection of personal data. • We do not penalise the DPO for performing their duties and ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO. Tasks of the DPO • Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits. • We will take account of our DPO's advice and the information they provide on our data protection obligations. • When carrying out a Data Protection Impact Assessment, we seek the advice of our DPO who also monitors the process. • Register (notify) under Data Protection Law with the ICO (excluding schools) • Our DPO acts as a contact point for the ICO. • When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing. • Our DPO can be contacted through: dataprotection@monmouthshire.gov.uk
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 to ensure that good GDPR 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. Managers must ensure that the Data Protection Officer is informed of any

	changes in their Service area's uses of personal data that might affect the organisation's Registration with the ICO. 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 their staff are aware of the mandatory GDPR training. (This will be monitored by Supervision and appraisal however, Individual officers are responsible for undertaking mandatory training as instructed. Should any breaches of the GDPR and related data protection law be identified, such as accidental or malicious loss of data, the individual's line manager must report the loss to the Data Protection Officer as soon as possible, without delay. In any event, data breaches that could result in harm to an individual must be reported by the Data Protection Officer to the ICO within 72 hours of the incident occurring or breach becoming known, following the breach flowchart process.

Staff	All staff and 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. Staff must familiarise themselves with the Mon CC GDPR video. Staff 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. In any case, at the start of employment, all staff must watch the introductory materials and be aware of: the key principles A-F, accountability, how to report a breach and where to find further information on GDPR compliance. This may be part of the Corporate Induction or Service/Volunteer level Induction (depending on which is first and ideally on the first day) Should any breaches of the GDPR and other relevant Data Protection law be identified, such as accidental or malicious loss of data, any member of staff must report the loss to their line manager as soon as possible, without delay who must then report to the Data Protection Officer. In any event, data breaches that could result in harm to an individual must be reported by the Data Protection Officer to the ICO within 72 hours of the incident occurring or breach becoming known.
Elected Members	All Elected Members 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 position. Elected Members must familiarise themselves with the Mon CC GDPR video. Elected Members 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. In any case, at the start of position, all Elected Members must watch the introductory materials and be aware of: the key principles A-F, accountability, how to report a breach and where to find further information on GDPR compliance. This may be part of the Corporate Induction or Service level Induction (depending on which is first and ideally on the first day) Should any breaches of the GDPR and other relevant Data Protection law be identified, such as accidental or malicious loss of data, an Elected Member must report the loss to the Data Protection Officer as soon as possible, without delay. In any event, data breaches that could result in harm to an individual must be reported by the Data Protection Officer or Elected Member (as a data controller in their own right) to the ICO within 72 hours of the incident occurring or breach becoming known. Elected Members are responsible for their own registration with the ICO as a data controller.
Volunteers	All 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. This will for example include being fully aware of the Team Kinetic Policy (content record management system), the electronic

	management system for linking volunteers with opportunities. Volunteers must familiarise themselves with the Mon CC GDPR video. 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. This will be recorded via Team Kinetic. In any case, at the start of a volunteering opportunity placement, all volunteers must use the introductory materials and be aware of: the key principles A-F, accountability, how to report a breach and where to find further information on GDPR compliance. This may be part of the Volunteer Induction or Service level Induction (depending on which is first and ideally on the first day) Should any breaches of the GDPR and other relevant Data Protection law be identified, such as accidental or malicious loss of data, volunteers must report the loss to the Volunteer Coordinator responsible as soon as possible, without delay. In any event, data breaches that could result in harm to an individual must be reported by the Data Protection Officer to the ICO within 72 hours of the incident occurring or breach becoming known.

Shared Resource Service (SRS)	The Shared Resource Service (SRS) is an arm's length joint service hosted by Torfaen County Borough Council that deals with MCC's Information Technology. The SRS is a collaborative ICT provision that covers Gwent Police, Monmouthshire County Council (MCC) and Torfaen County Borough Council (TCBC). The SRS is underpinned with a MOU (memorandum of understanding) that enables a single management structure across the board. **Services and responsibilities of the SRS:** ***Implementation Services***- providing MCC with development and technical programme services. Responsible for application development, implementation and transition through to project support. GIS (Geographic Information Services) application services and database services. ***Infrastructure Services***- server, airwave and network services. The server work stream is responsible for the deployment, implementation, management and support of the server infrastructure throughout the SRS. Responsible for the deployment, implementation, management and support of the network infrastructure through the SRS. ***Operations Services***- desktop services and operations services. Responsible for project support, frontline services support, installs, repairs and project work along with back office support. ***Information Security-*** ensuring that the SRS partners Networks are secured to the appropriate national standards. SRS takes ownership of the ISO27001 Accreditation for Ty Cyd 1 and manage the Technical and Physical Security of the SRS Partners.
Enforcement	Conduct, including negligence, which breaches GDPR and other Data Protection law 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 GDPR or other related Data Protection law 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 staff, volunteers, 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 GDPR, 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 Customer Relations in line with the Council's normal procedures, to ensure that exemptions or exceptions are applied correctly. Should any other department or school receive FOI requests direct they must centrally report to Customer Relations to receive a log number and follow normal procedure.
Confidentiality- code of conduct Confidentiality- exemptions	Access to confidential information will normally be on a "need to know" basis collected for specified, explicit and legitimate purposes and not further processed. The data will be limited to necessary purposes only 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 must provide new students and their parents GDPR complaint privacy notices before processing (including the sharing of) personal information. 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 appropriate exemption, which deals with matters of crime and taxation or safeguarding. Such information should only be released under the Council's Freedom of Information procedure or in the case of a GDPR Subject Access Request (SAR) with the agreement of the Council's Data

	Protection Officer, the Customer Relations Manager or another suitably empowered senior officer.
Privacy Notices (Fair Processing Notice)	Individuals are normally advised at the start of the relationship how their data will be used via a privacy notice. Some departments, such as schools and Social Services, use advisory leaflets as well as providing online links. Access our online Privacy Notice library. Personal data will be obtained either directly from an individual or indirectly. Where information has been received indirectly from another source, the source will be named along with the categories of personal information received.
Communication with staff, Volunteers and 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. Expected standards for Volunteers are set out in the Volunteer Agreement. The Council raises awareness with staff, volunteers and Elected Members via 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 Individual is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Individual 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 processing and retention	
General	The Council has developed policies and guidance for Data processing in relation to storage, security and appropriate deletion of personal data.
Information Asset Register "Systems list"	The Council maintains an information asset register known as the "Systems List" which sets out information such as: • the categories of personal data being processed, • the purpose of processing, • the legal basis for processing, • retention period and deletion methods, • links to privacy notice(s) • explicit consent (if applicable), • data protection impact assessments • ability to action individual rights such as the right to erasure • Third party contractor compliance
Retention periods	Retention periods for all types of documents are defined by the Council's Retention Schedule based on legislation and good practice.

6. Data Subject Access Requests (DSAR)

Responsibility	All officers are responsible for ensuring that any valid subject access request concerning information they hold are satisfactorily responded to within 28 calendar days. A request will not be considered valid until the identity of the requestor has been verified. An officer who receives a subject access request must contact the Data Protection Officer, who will oversee and expedite the process as necessary.
Procedure for making DSAR request	Subject access requests can be made verbally or in writing. Use of the subject access request form 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.
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. If applicable the right to data portability must be upheld, unless overridden by another lawful basis. 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 Elected Members' Welcome Packs

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 legitimately of use to another, or to a partner organisation through a recognised legal basis. (Explicit consent from the data subject, under contractual agreement, legal obligation, vital interests, undertaking a public task or acting under legitimate interests)
Legality	Data sharing is generally legal, provided that the provisions of the GDPR and other Data Protection Laws are satisfied. Data collected by Monmouthshire County Council may be shared with other relevant departments of the Council provided that there is a legal basis to do so and that the purpose for which the data is used is compatible with the purposes stated when the data was collected. (Transparently disclosed via data privacy notices covering the service) Specific guidance on responsibilities of Elected Members in relation to data protection laws can be found at www.ico.org.uk/for-organisations/political/ Any sharing with a partner organisation must also follow the GDPR and principles A-F and have a robust sharing protocol in place. If the GDPR 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 e.g. in a “life and limb” situation acting under Vital Interest. 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 the Information Sharing Protocol 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 £17million or 4% of gross annual turnover. 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. The GDPR imposes a strict deadline of 72 hours, from the time of the breach occurring or being identified to the time of the Data Protection Officer reporting the breach directly to the ICO. **CONCEALING OR FAILING TO REPORT A BREACH MAY BE CONSIDERED TO BE A DISCIPLINARY MATTER.**
Definition of breach	Personal data breaches can include: • access by an unauthorised third party; • deliberate or accidental action (or inaction) by a controller or processor; • sending personal data to an incorrect recipient; • computing devices containing personal data being lost or stolen; • alteration of personal data without permission; and • loss of availability of personal data.
Process to be followed	When a data breach is reported, the line manager or volunteer coordinator must promptly advise the Council's Data Protection Officer by telephone in the first instance. This must be followed up with an email to Dataprotection@monmouthshire.gov.uk providing relevant information, as requested by the DP Officer on the data breach. 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 (within the new timescale of 72 hours from time f breach occurring). Senior Information Risk Officer

	(SIRO) 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 register of all breaches and retain all relevant communications.
Complaints	If you object to the way that Monmouthshire County Council is handling your data, you have the right to complain. Please follow this link for further information on the complaints process. If you remain unhappy you also have a right to complain to the Information Commissioner's Office www.ico.org.uk

END

APPENDIX 1

List of related policies:

- Agile Working Policy
- Policy for Code of Conduct
- Digital Communications and Social Media Policy
- LA Retention Schedule
- MCC Information Security Policy
- MCC Non-Disclosure Agreement
- MCC Password Guide
- MCC Remote Access Policy
- Non-Disclosure Agreement for Volunteers/Contractors
- Standard terms and conditions for provision of services
- Terms and conditions for the supply of goods
- Volunteering Policy