DATA PROTECTION AND GDPR POLICY

YSGOL GYNRADD GATHOLIG PADARN SANT

Date Adopted: September 2021

Date of Review: September 2023

David Greaney, Chair of the Governing Body
Signed: David Greaney

CYNGOR SIR CEREDIGION COUNTY COUNCIL

Data Protection and GDPR Policy

2019

Document Control

Author and service: Corporate Lead Officer Customer Contact
Date approved by Cabinet: 19/02/2019
Publication date: 19/02/2019
Policy Review Date: February 2022

Date	Version	Author	Status
06/08/18	1.0	Patrycja Duszynska	First draft of the policy created to achieve compliance with new Data Protection Legislation
09/08/18	2.0	Arwyn Morris	First draft circulated and comments inserted.
31/12/18	3.0	CLO's	Final version agreed by CLO's
14/01/19	4.0	Arwyn Morris	Final version for Scrutiny
06/02/19	5.0	Scrutiny	Approved by Scrutiny
19/02/19	5.0	Cabinet	Approved

Contact Details:

Data Protection Officer

Phone: 01970633574 (-3573)

E-mail: data.protection@ceredigion.gov.uk

Contents

1 Definition of the policy

1.1 Purpose of the Policy

Ceredigion 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, residents of the County, job applicants and anybody who undertakes works on behalf of the Authority. The information we hold about them is their personal data.

Compliance with this policy will assist the Council in meeting the requirements of the European General Data Protection Regulation ('GDPR') and the accompanying Data Protection Act 2018 ('DPA').

This policy sets out how the Council seeks to protect personal data and ensure that staff and elected Members understand the rules governing their use of personal data to which they have access in the course of their work. All staff and elected Members must make themselves familiar with this policy and comply with its terms.

This policy also relates to the following legislative requirements incumbent on the Council:

Local Government Act 1972
Local Government (Access to Information) Act 1985
Freedom of Information Act 2000
Environmental Information Regulations 2004
Re-use of Public Sector Information Regulations 2005

This policy complements and sits alongside the following related Council policies:

Information and Records Management Policy
ICT Acceptable Use Policy
Information Security Policy
Freedom of Information Policy

The Information and Records Management Policy lays out the framework for the Council's records retention schedule, which is instrumental in adhering to the fifth GDPR data protection principle described below, that personal data should be kept for no longer than is necessary.

This policy sits alongside and complements the Council's privacy notice, which outlines how services within the Council collect and use personal data. The privacy notice lists individuals' rights to access and correct the data that is held on them, and in certain circumstances to object to its processing. The corporate privacy notice, which should be read in combination with this policy, is to be found at http://www.ceredigion.gov.uk/your-council/data-protection-freedom-of-information/data-protection/privacy-notice/

Failure to effectively implement this policy creates risks for the Council of non-compliance with legislation, significant monetary penalties from the Information Commissioner's Office (ICO), distress or harm to individuals whose data we hold, reputational damage to the Council and detriment to the Council's ability to deliver effective and reliable services.

1.2 Scope

This policy applies to all staff and elected Members who have access to Council records and information in whatever format in the course of their work. 'Staff' for these purposes includes permanent and temporary employees of the Council, volunteers and work experience interns, and external agents working for or on behalf of the Council.

This policy applies to all information held, maintained and used by the Council in all locations and in all media.

The responsibilities within this Policy extend to staff beyond their period of employment or to Elected Members beyond their period of office. This paragraph refers specifically to their continued responsibility to keep secure and not publicly disclose the personal data of any third party (particularly any sensitive personal information) to which they may have had privileged access by virtue of their period of employment or office.

1.3 Policy Definition

The following is a set of general definitions relevant to this policy. Some other definitions are given in the text where the term occurs and these can be identified by the emboldened text.

1.3.1 Personal Data

Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as school pupils or service users.

1.3.2 Special categories of personal data

Special category data means personal data consisting of information as to:

- Genetic and biometric data
- Political opinions
- Religious or other beliefs
- Trade union membership

- Physical or mental health/condition
- Sexual life

And although not specifically described as special category data, this information requires the same treatment:

- The commission or alleged commission of any offence
- Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings

1.3.3 Data Controller

Data Controller is a person or organisation who determines the purpose and manner in which any personal data are/or to be processed.

The Ceredigion County Council is a controller.

1.3.4 Data Processing

Processing data, means obtaining, recording or holding data. It also includes the carrying out of any operation on data, including:

- The organising, adapting or altering the data
- The retrieval, consultation or use of the data
- The disclosure of data by transmission, dissemination or otherwise making available
- The alignment, combination, blocking, erasure or destruction of the information or data

1.3.5 Data Processors

Data Processor is a person/organisation who processes data on behalf of a Data Controller and under their instruction.

1.3.6 Data Subject

Data Subject is the person whose personal information is held by a controller.

2 Principles of the Policy

The Council will implement technical and organisational measures to show that it has considered and integrated data protection into all its processing activities, in accordance with the applicable data protection principles, laws and rights of individuals as set out below in this section. The Council's approach to data protection will be, as required by GDPR, 'data protection by design and default' and 'privacy by design'.

2.1 Compliance with the six GDPR data protection principles

The Council will take steps to ensure that all the personal data processing it undertakes accords with the six data protection principles. These data protection principles are:

1) Personal data must be processed lawfully, fairly and transparently.
2) Personal data can only be collected for specified, explicit and legitimate purposes.
3) Personal data must be adequate, relevant and limited to what is necessary for processing.
4) Personal data must be accurate and kept up-to-date
5) Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
6) Personal data must be processed in a manner that ensures its security.

There is also an overarching principle of accountability which means that the Council must not only comply with the six GDPR principles but must be seen to be complying with them in its public face and be able to demonstrate compliance if inspected by regulatory bodies, such as the ICO.

2.2 First GDPR Principle: Fair and Lawful Processing

Processing of personal data must only be undertaken where the Council has a lawful basis for carrying out the activity. There are 6 potentially applicable lawful bases for general processing of Personal data and 10 lawful bases for processing Special Category Data. If Special Category Data is being processed, both a lawful basis for general processing and an additional condition for processing this type of data must be identified. These are listed in full in Appendix 1.

The legal basis for processing personal information for most of the Council's work will be carried out in the public interest or in the exercise of official authority vested in the controller;

The Council's legal basis for processing most 'special category' personal information will be necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2.3 Second GDPR principle: specified and legitimate purposes

When gathering personal data or establishing new data protection activities, staff should ensure that data subjects receive appropriate privacy notices to inform them how the data will be used. There are limited exceptions to this requirement, which are specified in GDPR. A 'privacy notice' is a statement that explains some or all of the ways an organisation gathers, uses, discloses, and manages the personal data it collects from its customers or clients. It fulfils part of the organisation's legal requirement to respect a customer or client's privacy when collecting and sharing personal data.

2.4 Third GDPR principle: adequate, relevant and limited

Staff should make sure data processed by them is adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should not generally be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

2.5 Fourth GDPR principle: accuracy

Individuals may ask the Council to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer (DPO).

2.6 Fifth GDPR principle: retention only as long as necessary

Personal data should not be retained for any longer than necessary. Staff should follow the corporate records retention schedule for guidance. The length of time for which data should be retained may vary from this schedule depending upon particular circumstances, including any special reasons why it was obtained.

2.7 Sixth GDPR principle: security

Staff must keep personal data secure against loss or misuse in accordance with the Information Security Policy. Where the Council uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the DPO to discuss the necessary steps to ensure compliance when setting up any new data processing agreement or altering any existing agreement.

2.8 Compliance with individuals' rights under GDPR

The Council will implement a set of rules and procedures, creating a workflow for the evaluation of requests, with regard to the following individual rights under GDPR:

1) The right to be informed
2) The right of access
3) The right to rectification
4) The right to restrict processing
5) The right to object
6) Rights on automated decision making and profiling
7) Right to data portability
8) Right to erasure or 'right to be forgotten'

2.9 The right to be informed

The Council will explain at the point of collection how it intends to use the data it is collecting, whether it will share the data with anyone else, what the legal basis for processing is and which individual rights apply. The primary method for communicating this information will be the corporate privacy notice,

supplemented by brief privacy statements at the point of collection which reference amongst other things the full notice. Other versions of the privacy notice will complement it, suitable for explaining the concepts of privacy and data protection to children and to others who may reasonably expect the information to be available in other, more accessible formats.

2.10 The right of access

Individuals are entitled (subject to certain exemptions specified in the Data Protection Act) to request access to information held about them. All such Subject Access Requests should be logged at a corporate level and referred onward immediately to the relevant officer(s) for action. Timeliness is particularly important because the Council must respond to a valid request within legally prescribed time limits.

2.11 The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. The Council must respond within one month to any reasonable request for rectification, although this can be extended by two months where the request for rectification is complex. If the Council has shared the personal data in question with other agencies, each agency must be informed and asked to make the same rectification - unless this proves impossible or involves disproportionate effort. If asked to, staff must also inform the data subjects about these agencies whose data may also be inaccurate. If the request for rectification is refused (for example where the data subject's authenticity is contested), staff must explain why to the individual, informing them of their right of appeal to the DPO and to seek a judicial remedy.

2.12 The right to restrict processing

Individuals are entitled to block the processing of their personal data in certain circumstances. The data may continue to be stored but processing of it must cease. The Council is only required to restrict the processing of personal data in the following circumstances: where an individual contests the accuracy of the personal data; where following an objection to processing the Council is considering whether its legitimate grounds override those of the individual (this is only applicable where the legal basis for processing is either performance of the public task or the exercise of legitimate interests, see 2.13 below); when processing is unlawful and the individual opposes erasure and requests restriction instead; if the Council no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

2.13 The right to object to processing

Where the legal basis for processing is performance of a public task or the exercise of legitimate interests, individuals have the right to object to processing, including any profiling based on those provisions. The Council shall no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. Where the legal basis for processing is consent, individuals have an absolute right to object to the Council

processing their data for this purpose, to which demand staff must immediately respond without question. This legal basis for processing and this right applies in particular to any direct marketing undertaken by the Council, for example marketing for its cultural, leisure and other discretionary/optional services.

2.14 Rights on automated decision making and profiling

Individuals have the right to be informed when their data is subject to automated decision making and profiling. The Council does not currently carry out such activity, hence the condition does not apply at present.

2.15 Right of portability

Individuals have the right to demand that their personal data is transferred to another agency (for example when moving to another area). It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This limited right only applies where the legal basis for processing is performance of a contract or based on consent, hence is not applicable in any great degree to local authorities.

2.16 Right to erasure or 'right to be forgotten'

Individuals also have the right, in the case of reliance on consent, to demand that their personal data be removed entirely from the particular processing activity, the so-called 'right to be forgotten'. This limited right applies mostly to direct marketing activity by the Council.

3 Implementation of the policy

The Council will take the necessary actions to ensure that it complies with all other legal obligations imposed on it by GDPR and the Data Protection Act. Specifically, this involves appointing a DPO, maintaining a Register of Processing Activities; maintaining a record of consent; undertaking Data Protection Impact Assessments; promptly investigating data breaches; not transferring personal data outside the European Economic Area and other countries designated as having an adequate level of data protection regulation.

The existence of an information governance structure within the Council in no way negates or reduces the individual accountability and responsibility of all staff and elected members for protecting the personal data to which they have access.

3.1 Register of Processing Activities

The Council will maintain a **Register of Processing Activities** (within the Council this will be known as the Information Asset Register) which will record all data processing activity undertaken by the Council, amongst other things

defining the legal basis for each activity, the categories of data contained within each system and identifying cases where the Council shares the data and with whom.

3.2 Maintaining a record of consent

Where the legal basis for processing is consent, the Council must explain why the data is being collected, how it will be processed and whether it is to be shared with anyone else, before obtaining the data subject's consent. Consent of this type is usually gathered through a tick box, which cannot be pre-ticked. A record must be made and maintained of the data subject's consent.

Where the legal basis for processing is consent and the categories of data to be collected include sensitive personal data, it will be necessary to have an individual's explicit consent to process sensitive personal data, unless exceptional circumstances apply. Explicit consent of this type is usually gathered through a signature obtained below a clear privacy statement. A record must be made and maintained of the data subject's explicit consent.

3.3 Data Protection Impact Assessments

A '**Data Protection Impact Assessment'** is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system containing personal data. The Council must carry out Data Protection Impact Assessments when, for example, building new systems for storing or accessing personal data; developing policies or strategies that have privacy implications; embarking on a data sharing initiative; or using data for new purposes. An assessment is required where new or changed processing involves large amounts of personal data, where new regional partnerships or commercial outsourcing involve the transfer of personal data to third parties, or in the case of a data breach which brings to light risks in existing methods of processing.

In determining whether a Data Protection Impact Assessment is necessary, they must consult the DPO for advice. The completed assessment must be submitted to the DPO and stored as part of the Information Asset Register (Register of Processing Activities).

3.4 Data breaches

In the event of a Data Breach the DPO will carry out an assessment to determine whether the data subject and/or the ICO should be informed of the breach. If required the ICO will be informed within the 72-hour timeframe as prescribed by GDPR.

3.5 Transfers of data outside the European Economic Area (EEA)

There are restrictions under GDPR on international transfers of personal data outside the EEA because of the need to ensure that adequate safeguards are in place to protect it. Staff unsure of what arrangements need to be put in place before transferring data outside the EEA should consult the DPO.

3.6 Information Sharing

The Data Protection Act is not a barrier to sharing information but rather provides a framework to ensure that personal information about living persons is shared appropriately. Staff should not hesitate to share personal information in order to prevent abuse or serious harm, in an emergency or in life-or-death situations. If there are concerns relating to child or adult protection issues, then the relevant procedures should be followed.

The Wales Accord on the Sharing of Personal Information (WASPI) was developed as a practical approach to multi agency sharing for the public sector in Wales, to which the Council signed up in June 2011.

Information sharing is key to joined-up service delivery. Decisions on whether to share information must be taken on a case-by-case basis which should then be supported by the production of either an Information Sharing Protocol (ISP) or a Data Disclosure Agreement (DDA).

Each ISP and/or DDA must have a clearly defined purpose for the sharing and must be seen and registered by the IRM Service before being signed off at Corporate Lead Officer level.

3.7 Protection of children and vulnerable people

Where information is passed to the Council concerning safeguarding, then the risk posed and the individual's right to privacy will have to be balanced against each other.

If information received by the Council relating to any person(s) who may come into contact in any way with children and/or vulnerable persons raises concerns as to the appropriateness of the person(s) having contact with children and/or vulnerable people and/or as to the future well-being of such children and/or vulnerable persons, the Council will consider it a duty to share that information. It may be shared with any appropriate individual, company group, committee, Police Force and other Council or agency if the balance of risk is deemed to require the sharing of such information.

3.8 Data Protection Officer

The Council must have a Data Protection Officer with overall responsibility for the Council's adherence to this policy. The DPO will report to the Senior Information Risk Owner (SIRO) and Monitoring Officer.

3.9 Corporate Lead Officers

Corporate Lead Officers are responsible and accountable for maintaining appropriate procedures and standards of data protection within their service unit. The requirements of this policy will be acknowledged and included in each service unit's business plans, along with the related issues of information management, records retention, and compliance with Freedom of Information requests.

Corporate Lead Officers will ensure that all staff within their service unit:

- Are aware of their responsibilities for data protection, for example by monitoring the compliance of their staff with mandatory data protection training;
- Do not enter into contractual arrangements which do not comply with the requirements of GDPR with appropriate clauses about data protection and privacy.
- Know where to look and who to approach for advice and guidance on the subject of data protection.
- Ensure that staff are appropriately trained to the correct level and have signed appropriate undertakings in certain cases where highly sensitive personal data is processed, in order to protect and responsibly manage the personal data to which they have access through their employment.

3.10 Council Staff

All staff are responsible and accountable for following established corporate and departmental procedures with regard to data protection and for keeping their training and understanding up-to-date and in particular for undertaking all mandatory training. Corporate guidance to staff for the proper management and protection of personal data will be created, maintained and disseminated through the staff intranet and through other appropriate means to those staff who do not have access to the intranet. Failure to comply with this policy and the principles set out in the Act will be regarded as serious misconduct and will be dealt with in accordance with the Council's disciplinary policy. Misuse and unauthorised disclosure of personal data can lead to personal prosecution. All staff are also responsible for ensuring that volunteers, apprentices, trainees and work experience interns working alongside them temporarily are given, where necessary, an appropriate basic training as part of their induction about data protection and respect for individual privacy rights.

3.11 Councillors

All elected members are responsible and accountable for following established procedures and keeping their training and understanding up-to-date with regards to data protection. Corporate guidance to elected members for the proper management and protection of personal data will be created, maintained and disseminated through the Council's intranet and through face to face training.

4 External advisory standards affecting this policy

This policy is informed by the ICO's guidance on the implementation of GDPR. The guidance can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

This policy will be reviewed and if necessary amended following any revision by the ICO in its guidance and/or any significant legal case interpreting GDPR or the Data Protection Act especially in so far as it might affect the responsibility of public authorities.

5 Policy Monitoring and Review

Effectiveness of the implementation of the policy will be assessed at intervals by internal audit and/or the DPO, who may carry out an internal investigation without prior notice or consent.

Such audits of service areas may, amongst other measures:

- Identify areas of operation within the service area that are covered or not covered by the policy and to identify any relevant processing and/or procedures which fail to adhere to the policy
- Demand that a Data Protection Impact Assessment be carried out immediately where current methods of data processing present a corporate risk (for example where large quantities of sensitive personal data are being processed with potentially inadequate safeguards), or where a significant data breach has already occurred.
- Set requirements for implementing new operational procedures with regard to data protection, processing of data and dealing with requests for information.
- Identify where non-compliance with the operational procedures is occurring and suggest appropriate adjustments in the form of an improvement action plan

The SIRO and DPO will formally review the policy annually and amend if necessary. The amended policy will be distributed to all staff.
The policy will be reported to Council on a 5 yearly basis or when significant changes are made.

Appendix

GDPR specifies six lawful bases for processing, as follows:

1) Processing is necessary for compliance with a legal obligation to which the controller is subject. This is applicable to all statutory services which the Council is obliged to provide.
2) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is applicable to all services where the Council is empowered but not obliged to provide a service by legislation (for example the provision of council housing).
3) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
4) Processing is in the vital interests of the data subject.
5) Processing is in the Council's legitimate interests and does not unduly prejudice the individual's privacy. This is applicable only to internal services such as Payroll and HR and cannot be applied to the Council's public task.
6) The data subject has given consent to the processing of his or her personal data for one or more specific purposes. This is applicable mostly to marketing activity.

10 legal bases for processing Special Category Personal Data:

1) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes;
2) processing is necessary for the purposes of carrying out the obligations and rights of the data controller or of the data subject in the field of **employment and social security** (subject to the Data Protection Act 2018);
3) processing is necessary to protect **the vital interests of the data subject** or of another natural person where the data subject is physically or legally incapable of giving consent;
4) processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5) processing relates to personal data which are **manifestly made public by the data subject**;
6) processing is necessary for the establishment, exercise or **defence of legal claims** or whenever courts are acting in their judicial capacity;
7) processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and

specific measures to safeguard the fundamental rights and the interests of the data subject;

8) processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to safeguards;
9) processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016
10) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.