Cyngor Abertawe
Swansea Council

Data Protection Policy

Document Control

Title	Data Protection Policy
Author	Kim Collis
Owner	Data Protection Officer
Protective Marking	[UNCLASS]

Revision History

Revision Date	Version	Previous Version	Description of revision
28/03/2018	1.0	Draft	Minor change requested by CMT
2/10/2019	2.0	1.0	Refresh

Contents

Page

1. Purpose of the Policy

1.1 Swansea Council ('the Council') holds personal data about its citizens, employees, suppliers, job applicants and other individuals for a variety of business purposes, including its public task as a local authority, its status as a major local employer and as a commissioner of services.

1.2 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.

1.3 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. 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

1.4 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.

1.5 The Council may supplement or amend this policy by additional policies and guidelines from time to time.

2. Scope of the Policy

2.1 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 Swansea Council, volunteers and work experience interns, and external agents working for or on behalf of the Council.

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

2.3 Some of the responsibilities within this policy extend to employees of the Council 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.

3. Definitions

3.1 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.

- '**Data**' is a set of values of quantitative or qualitative variables and can be of many types.
- '**Personal data**' means any data relating to living individuals from which they can be identified, either directly from the data itself or by another individual when combined with other data that is in, or likely to come into, their possession. Personal data includes any data which includes expression of opinion about the individual and any indication of someone else's intentions
- A '**Data subject**' is an identified or identifiable individual whose personal details are contained in the data.
- '**Processing**', means here obtaining, recording or holding information or data, or carrying out any operation or set of operations on that information or data, including its organisation, retrieval, disclosure, combination with other data, or destruction. It primarily refers to activity carried out by computer systems, although some manual processes may qualify as processing if the data is highly structured and can be manipulated manually to produce meaningful items or sets of data.
- **'Business purposes**' means the purposes for which personal data may be lawfully used by the Council, for example administrative, regulatory, financial and business development use
- A '**data controller**' is an organisation or individual that determines the purposes and means of processing personal data.
- A '**data processor**' is responsible for processing personal data on behalf of a data controller. In many if not most cases, the data controller and data processor are the same organisation or individual. In some cases, Swansea Council uses a third party to process the data it collects, for example for commercial reasons
- A **'joint data controller**' is where two or more controllers jointly determine the purpose and means of processing. This situation may arise where the Council is collecting the data on behalf of a larger regional or pan-Wales partnership.
- '**Sensitive personal data**' is data which reveals an individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sex life. The presumption is that, because information about these matters could be used in a discriminatory way and is likely to be of a private nature, sensitive personal data needs to be treated with greater care than other personal data.

4. Context of the Policy

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

Information Management Policy
Records Management Policy
ICT Acceptable Use Policy
ICT Security Policy
Staff Data Storage Policy
Corporate Risk Management Policy

4.2 The 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.

4.3 This policy sits alongside and complements the Council's privacy notice, which outlines how departments 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 https://www.swansea.gov.uk/privacynotice

5. Principles of the Policy

5.1 The Council will implement technical and organisational measures to manifest 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'.

5.2 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 as described in Article 5 of GDPR. 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 furthermore 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.

5.3 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. 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.

5.4 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.

5.5 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.

5.6 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).

5.7 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.

5.8 Sixth GDPR principle: security

Staff must keep personal data secure against loss or misuse in accordance with the ICT Security Policy Framework. 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.

5.9 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'

5.10 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 is the legal basis for processing 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.

5.11 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.

5.12 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.

5.13 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 5.14 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.

5.14 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.

5.15 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. A note to this effect is contained in the privacy notice.

5.16 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.

5.17 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.

5.18 Compliance with other legal obligations under GDPR

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.

5.19 Data Protection Officer

The Council will appoint or designate the role of Data Protection Officer within the authority, who will monitor internal compliance with the legislation, inform and advise the Council on its data protection obligations, provide advice regarding Data Protection Impact Assessments and in certain instances act as a contact point between data subjects and the Council.

5.20 Register of Processing Activities

The Council will maintain a Register of Processing Activities (within the Council this is known as the Information Asset Register) which records 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 we share the data and with whom.

5.21 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.

5.22 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 will carry out Data Protection Impact Assessments when, for example, building new systems for storing or accessing personal data; developing policy or strategies that have privacy implications; embarking on a data sharing initiative; or using data for new purposes.

Such an assessment is likely to be required where new or changed processing involves large amounts of sensitive 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, officers will either decide this themselves, guided by the screening mechanism available on the staff intranet (which involves the completion of a series of questions, the answers to which lead to a recommended course of action) or they may consult the DPO for advice where further clarity is needed.

They may also be mandated by the DPO to carry out the assessment. The completed assessment should be scrutinised and certified by the DPO and stored as part of the Information Asset Register (Register of Processing Activities).

5.23 Data breaches

The Council will implement rules and procedures to ensure that it is able to respond to data breaches within the 72-hour timeframe prescribed by GDPR, the investigatory panel carrying out an assessment to enable it to determine whether the data subject should be informed of the breach and/or the ICO notified.

5.24 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.

At present, the Council does not transfer personal data outside the EEA in a systematic fashion, other than using the Privacy Shield to transfer data to the USA (the adequacy of the Privacy Shield is under review).

6. Responsibilities for implementing the policy

6.1 The Council will appoint a Data Protection Officer with overall responsibility for the Council's adherence to this policy. The DPO will be complemented by the roles of Senior Information Risk Owner (SIRO) and deputy SIRO.The DPO will ensure compliance with the eight data protection principles of GDPR, in particular when any new data processing activity is initiated or any accidental loss or damage to data occurs.

6.2 These positions will be supported by an Information Governance framework which will be subject to periodic review for its effectiveness, but will comprise at its most basic level a network of representatives from each of the service units within the organisation. 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.

6.3 Each Head of Service will be the senior officer with responsibility for maintaining appropriate procedures and standards of data protection within his or her service unit, as guided by the DPO and staff involved in information governance.

The requirements of this policy will be acknowledged and articulated in each service unit's business plans, along with the related issues of information management, records retention, and compliance with Freedom of Information requests.

6.4 Heads of Service 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, privacy and so forth;
- 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.

6.5 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 (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

6.6 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.

6.7 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.

7. External advisory standards affecting this policy

7.1 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.

8. Monitoring of compliance

8.1 The Council should follow this policy for all relevant processes and procedures in its operational activities. Effectiveness of the incorporation of the policy into departmental processes and procedures will be assessed at intervals through the process of internal audit and at the behest of the DPO, who may carry out an internal investigation without prior notice or consent should s/he have cause for concern. Such audits of service areas will, 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.
- Highlight where non-conformance to the operational procedures is occurring and suggest a tightening of controls and adjustment to related procedures in the form of an improvement action plan

9. Policy Review

9.1 The Council will keep this policy under continuous review, amending it when necessary and formally reviewing it at intervals of not more than five years.
Policy due for review April 2021