Gwybodaeth dan Reolaeth

Gwynedd Council

DATA PROTECTION POLICY

3.0

June 2018

Information Management Service

1. Introduction

In undertaking its work, the Council will create, gather, store and process a large amount of personal information about members of the public, staff, customers, service users and others.

Therefore, it is necessary to adhere to data protection legislation – the General Data Protection Regulation 2016 and the Data Protection Act 2018.

2. Purpose

The purpose of this policy is to set out the responsibilities of the Council and its staff to comply fully with data protection legislation.

3. Scope

Compliance with the legislation and adhering to the policy and principles as outlined below is the responsibility of all members of staff. Further information and guidance can be found on the intranet.
Any deliberate breach of the policy may lead to disciplinary action or even a criminal prosecution.

4. Personal and Sensitive Data

Personal data is information about a living individual who is identifiable from that information.

Sensitive information is classified as 'special category' data (Appendix 1) and particular care must be taken when using this data.
This is information relating to:

Race, ethnicity, health, political beliefs, trade unions, biometric or genetic information, religion, sexual life or sexual orientation.

5. Principles

In simple terms, the Council is required to adhere to the principles of data protection.

According to Article 5 of the GDPR:

a) Information must be processed lawfully, fairly and in a transparent manner

b) It must be collected for specified purposes and not used in a manner that is incompatible with those purposes

c) Personal data must be adequate, relevant and limited

d) Data must be accurate and kept up to date

e) It must not be kept for longer than is necessary

f) It must be processed in a manner that ensures appropriate security of the data

6. Lawful Conditions for Processing

In order for it to use personal information, the Council must have a lawful basis. In addition, the processing of sensitive information requires additional processing conditions.
These are noted in Appendix 1.

The Council will document the lawful basis of processing for its activities and inform individuals via its privacy notices.

7. Consent

Consent is only one of the conditions for processing. As the Council is a public authority, it is unlikely that consent will be appropriate as a lawful basis for processing and therefore, where possible, alternative justification should be used (e.g. official authority or contract).

Where consent is used, it must be freely given, specific, informed and unambiguous. Silence, pre-ticked boxes or inactivity does not constitute consent.

8. Privacy Statements

Under the fair and transparent requirements of the first data protection principle, the Council is required to provide individuals with a privacy notice to let them know what it does with their personal information.

A template is available on the intranet.

9. Data Retention

Personal information should not be kept for longer than is necessary. If it is no longer required, it must be disposed of securely, or deleted (if in electronic form).
Please contact the Information Management Service for information about our retention periods.

10. Record of Processing Activities

The Council will maintain a record of activities in the form of an information asset register. This will note why the personal data is being processed, details about the data, where it is held, who it is shared with, the lawful basis, and security measures to safeguard the information.

11. Individual Rights

Right of Access

Individuals can request to see any information that the Council holds about them which includes copies of email correspondence and any opinions expressed about them.

The Council will respond to such requests for personal information in accordance with its data handling procedures.

In order to comply with the requirement to treat English and Welsh on an equal basis, the Council will provide any summaries of Welsh language materials in English but will ask the applicant to arrange a full translation themselves.

Right to erase, to restrict processing, to rectify, portability and the right to object

Individuals also the above-noted rights. See Appendix 2 for further details.

If a staff member receives such a request, it should be referred to the Data Protection Officer immediately.

Rights in relation to automated decision making and profiling

See the information in Appendix 2

12. Data Sharing

If we share date outside the Council, there must be a lawful basis for the sharing and the individual should have been informed of the identity of the third party.

When collaborating with certain partners, the Council has entered into information sharing protocols and data disclosure agreements under the Wales Accord on Sharing Personal Information framework.

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 procedure should be followed.

Disclosing information to councillors

Reference should be made to Section 3 “Obtaining Information and Participating” and Section 14 “Procedural Guidelines on Access to Information” in the Constitution. Occasionally, a member will ask for information on behalf of his/her electors. On such occasions, in order to avoid any confusion, members are encouraged to obtain the elector’s written consent for information about him/her to be revealed to the member. Decisions about the right of councillors to personal information are made on a “need to know” basis and any case in which there is doubt should be referred to the Monitoring Officer.

Requests from Outside Bodies

Outside organisations may ask the Council to disclose personal information that the Data Protection Act provides an exemption for, such as organisations that process personal information for the purposes of crime detection and prevention or collection of taxes or duties.

Requests to other organisations

Additionally, some services within the Council (e.g. Taxation Unit, Benefits) also have the right to request information and therefore they too should follow the appropriate procedures to obtain this information.

Data processing agreements

Where a commercial relationship exists which means that a third party is processing personal data on behalf of the Council, and is operating as a 'data processor', a written contract must be in place that includes the conditions set out in the GDPR.

13. Data Protection by Design

Under the GDPR and the Data Protection Act, the Council has a duty to consider the impact of each data processing activity on data protection.

Data Protection Impact Assessments

When considering new activities that involve processing personal data, or when establishing new procedures or systems that involve personal data, the impact on privacy must be considered at the outset. A Data Protection Impact Assessment should be undertaken.

The purpose of the assessment is to identify any risks to privacy and personal information at the beginning of any activity or project.

The Council will undertake such Assessments when it is required to do so. A template is available on the intranet.

14. Data Security

Each user is responsible for ensuring that personal information is always secure, and that it is not disclosed to an unauthorised third party unintentionally, through negligence or intentionally.

The Information Security Operational Procedure should be read in conjunction with this Policy.

Data Security Breaches

A data breach means a situation where information is lost, destroyed or unintentionally damaged.

Any incident in which personal information is disclosed (whether intentionally or unintentionally) must be reported to the Council's Information Manager *immediately.*

The Officer will decide whether or not the breach is sufficiently serious, and if it is, it must be reported to the Information Commissioner's Office as soon as possible, and within 72 hours of becoming aware of it.

15. Responsibilities

Staff Members

All staff members have a responsibility to ensure that they adhere to the principles and other conditions of the legislation. A clause in each job description clearly states this responsibility.

Information Asset Owners (service managers)

- Ensure that the record of processing activities is kept up to date.
- Ensure that their staff receive a level of training appropriate to their job.
- Ensure that staff read and accept all data protection related policies.
- Ensure that the personal information for which they are responsible is shared appropriately internally and externally.
- Ensure that access to electronic folders and files and paper files is strictly controlled.

Senior Managers

Undertake specific overview functions within their department in the fields of data protection.

Heads of Service

Overall responsibility for compliance within their service.

Data Protection Officer

- Provide advice
- Provide training
- Administer the complaints procedure
- Undertake audits
- A single point of contact for the public and the Information Commissioner's Office.

Information Management and Security Group

The group includes a representative of each department and is chaired by the Head of the Corporate Support Department.
The purpose of the group is to act as a contact point for the departments for matters relating to information, and to note any risks that need to be drawn to the attention of the Head of Corporate Services, who is also the Council's Senior Information Risk Owner.

16. Complaints

If a complaint is received from the public about the Council's use of personal information, the matter should be dealt with by the Data Protection Officer.

Similarly, the attention of the Data Protection Officer should be drawn to any example of failure to comply with the Act or the guidelines.

17. Non-compliance

All staff are required to comply with the policy and any member of staff who is found to have made an unauthorised disclosure or breached the terms of the policy may be subject to disciplinary action.

The Council could be fined for non-compliance, up to 10million euros or 20million euros, depending on the nature of the infringement.

18. Contact points and further information

The Head of Corporate Support is the Council's SIRO (Senior Information Risk Owner) and therefore has responsibility and accountability at senior level.

The Council's Data Protection Officer is Helen Parry, Information Manager, dataprotectionofficer@gwynedd.llyw.cymru.

Further details can be found on the Information Commissioner's Website - www.ico.org.uk

19. Review

This policy will be reviewed in two years' time.

Appendix 1

The processing of any personal data must be justified. One of the following conditions must be met:

1. The individual has given consent
2. Processing is necessary for the performance of a contract
3. Processing is necessary for compliance with a legal obligation
4. Processing is necessary to protect vital interests
5. Processing is necessary to for the performance of a task that is in the public interest or in the exercise of the organisation's official authority
6. Processing is necessary for the purposes of legitimate interests

In relation to sensitive data, one of the following conditions must **also** be met:

(a) The individual has given consent

(b) processing is necessary for the purposes in the field of employment and social security and social protection law

(c) processing is necessary to protect vital interests

(d) processing is carried out by a foundation, association or any other not-for-profit body

(e) processing relates to personal data which are made public by the individual;

(f) processing is necessary for the establishment, exercise or defence of legal claims

(g) processing is necessary for reasons of substantial public interest

(h) 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

(i) processing is necessary in the area of public health, such as protection

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, providing suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2

Right to Object

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

The Council will stop processing the personal data in question unless

- It can demonstrate compelling lawful basis for the processing, which override the interests, rights and freedoms of the data subject; or
- the processing is for the establishment, exercise or defence of legal claims.

Right to erasure

This provides individuals with a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of online information services to a child.

The Council can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes, or
- The exercise or defence of legal claims.

Right to restrict processing

When processing is restricted, the Council can store personal information but not process it.

Where an individual has contested the accuracy of their data, the processing should be restricted until the accuracy has been verified.

- Where a data subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and consideration is being given to whether the Council's lawful basis overrides those of the data subject.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If the information no longer needs to be held but the data subject requires the data to establish, exercise or defend a legal claim.

Right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The Council will have one month (which can be extended to two if the rectification is complex) to respond to such a request and, if a decision is taken not to take action, the individual will be given the reasons why and the right of complaint to the Information Commissioner's Office and to judicial remedy.

The Council will inform any third parties of the rectification where possible and will also inform the individual about the third parties to whom the data has been disclosed where appropriate.

Rights in relation to automated decision making and profiling

Profiling is the processing of data to evaluate, analyse or predict behaviour. Automated decision making involves decision making without any human involvement.

There are additional rules if the Council is carrying out automated decision making that has legal effects on the individual.

The Council will document the legal basis for the above and inform individuals when either profiling or automated decision making is taking place.

Right to portability

The individual may request that information is provided in a structured, commonly used and machine readable format in order to be sent to another organisation. This right only applies in certain circumstances.