Gwybodaeth
Dan
Reolaeth

Gwynedd Council

DATA PROTECTION POLICY

FINAL 2.0

September 2015

Information Management Service

CYNGOR GWYNEDD COUNCIL

Approved 2015 07 22

1. Introduction

The Council makes considerable use of personal information in all its fields of work from council tax to planning applications and therefore it is important that it adheres strictly to the Data Protection Act 1998 ("the Act").

The purpose of this policy is to explain what is required of the Council and its staff.
The Council has designated one of its officers as Data Protection Officer but each and every member of staff is required to adhere to this policy and the principles of the Act.

Failure to comply with the Act is a serious offence - the individual can be prosecuted as well as the Council.

2. The Act

In simple terms, the Act requires that we:

- Keep personal information secure
- Ensure that information is used appropriately
- Ensure that individuals know what organisations are doing with their personal information
- Ensure accuracy
- Ensure that only the minimum amount of information is processed and that it is not kept for longer than necessary

3. Staff Responsibilities

The Act places responsibility on the individual as well as the authority. It is possible for an individual member of staff to be prosecuted for failing to comply with the Act. As part of his/her employment with Gwynedd Council every member of staff is expected to be familiar with his/her data protection responsibilities and to deal with personal information in a manner that complies with the Act. Every member of staff must therefore read and follow this policy.

Failure to comply with these guidelines could lead to disciplinary action.

Noted below are the Council's expectations of its staff.

- All staff, not just those coming face to face with customers, must read and understand the Data Protection Policy and understand their responsibilities under the Act.

- All staff must have attended an appropriate training session on Data Protection, completed the e-learning module or be sufficiently aware of the act in accordance with the requirements of their post.

- All staff must comply with the Information Security Policy, which is available in the Policy Centre

- All staff must be able to identify personal information and to deal with it in accordance with the guidelines in the policy.

- All staff must familiarise themselves with the sets of personal data within their department. In particular, staff who are responsible for keeping personal information must ensure that their manager knows of the existence of that information.

- Where there is doubt regarding data protection, any question should be referred in the first instance to the department's senior manager.

- If there is any doubt regarding the right to disclose information, advice should be sought first.

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

- Where there has been a serious breach of the Act, the Council may decide to report the incident to the Information Commissioner. The Information Commissioner has the power to impose fines of up to £500,000 on organisations.

Principle 1 – Lawfulness and Fairness

In order to process *personal data* **lawfully**, there must be some reason or justification. This means meeting one of the conditions listed in the Act (see appendix 1) e.g. consent of the individual, for the performance of a contract, administration of justice.
Particular care must be taken with *sensitive personal data*, and as such, the conditions for processing are much stricter (see appendix 1 again)

To satisfy the requirements of **fairness,** individuals should be informed **who** is processing their data and what **use** will be made of it. All forms used for the collection of personal information should therefore contain an appropriate notice under the Act e.g.
Data Protection Act 1998: Gwynedd Council is the data controller for the purposes of the Act. The information on this form will be used for the purposes of [xxxxxxxxxxx].

Information may be shared between services where this is compatible with the Act.

Principle 2 – Specified Purposes

Before collecting personal data, decide what it's going to be used for.

The reason should be set out on any paper work together with the details of any company/authority/agency with whom the data will be shared.

Data used for one purpose should not be used for a completely different purpose without the consent of the individual.

Principle 3 – Adequate, Relevant and Not Excessive

Data should only be kept for the purposes which the individual has been notified about.

Principle 4 – Accurate and Up to Date

Data should be accurate, and where necessary, kept up to date by carrying out regular system checks

Principle 5 – Not Kept for Longer than Necessary

Data may only be kept while they are needed for a specific purpose.

When the purpose no longer applies, the data should be deleted.

Use should be made of the corporate retention periods which set out how long different records should be kept – the Records Management Team can provide assistance in this respect.

Principle 6 – Rights of Individuals

The rights of individuals include the right to write to the Council to find out what information is stored about him/her. Staff must be able to access records easily to respond to such requests (which include e-mail records).

Such applications should be referred to the Information Manager.

Principle 7 – Keeping information secure

Personal information must not be disclosed (orally or in written form) to any unauthorised third parties,

Access to personal information should be limited those who absolutely need to know.

All personal information should be kept securely under lock and key.

A clear desk policy should be adopted i.e. paper files should not be left out on desks. The Information Management Team will be carrying out spot checks to ensure that staff adhere to this policy.

Personal information should be disposed of by shredding or other appropriate secure methods – in accordance with the Confidential Waste Disposal Policy.

When transferring data to another organisation for processing, there should be a written contact between the Council and the organisation – contact the Legal Unit for advice.

Any personal data taken off the premises poses a considerable risk, therefore particular care must be taken e.g.,

- Personal information should only be taken home when absolutely necessary and for the shortest possible period.

- Personal information should not be kept in vehicles overnight.

4. Responsibilities of Managers

Ensure that their staff receive a level of training appropriate to their job.

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.

5. Responsibilities of Heads of Departments

In order to ensure that the Council's data protection arrangements work effectively individual departments will need to have procedures on how to deal with various data for which they are responsible. In particular, it is necessary for departments to have the following:

- Every head must ensure that staff receive appropriate information and training on their data protection responsibilities.

- Every head must have guidelines noting for how long various records/data will be kept within their department. These will be based on corporate guidelines.

- Every head must have a procedure to verify data and to ensure that it is current. This will mean either a procedure to check information when it is received (unless it comes from the individual who is the subject of the data) or a procedure to carry out occasional checks of all the data in a series. (In general, it is thought that 3 years is a suitable period).

- Every head must have a procedure to ensure the security of personal information. This will include guidelines on who has a right

of access to personal information, where and how it is kept, and guidance on physical security.

- Every head must ensure that they know what personal information is kept within their department and who is the person responsible for it. This will mean identifying computer and paper systems that include personal data in accordance with the definition in the Act.

- Staff, managers and heads should question continuously whether there is a real need to print/retain/receive/share or transport personal information.

6. Requests for personal information

6.1. Individuals

The Council will respond to requests for personal information under the Act in accordance with the procedure set out in the relevant guidelines. We must respond within 40 calendar days and a fee of £10, the maximum, will be charged.

6.1.1 Translation

Section 7(1)(c) of the Act states that information must be provided in an 'intelligible' form. In order to comply with this requirement and 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.

6.2 Disclosure of 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.

6.3 Requests from Outside Bodies

Outside organisations may ask the Council to disclose personal information – Section 29 of the Act provides an exemption for organisations that process personal information for the purposes of crime detection and prevention or collection of taxes or duties. Should such applications be received e.g. from organisations such as the HM Revenue and Customs or the Police, they should be directed to the Information Manager.

6.4 Requests to other organisations

Some services within the Council (e.g. taxation unit, benefits) also have the right to request information under Section 29 and therefore they too should follow the appropriate procedures to obtain this information.

7. Complaints

It is essential to deal with complaints effectively. If a complaint is received from the public about the Council's use of personal information, the matter should be dealt with through the official complaints procedure, whilst at the same time bringing it to the attention of the Information Manager. Similarly, the attention of the Information Manager should be drawn to any example of failure to comply with the Act or the guidelines.

8. Other relevant policies

This policy is to be read in conjunction with the following:

- Information Management Policy
- Information Security Policy
- Confidential Waste Disposal Policy

9. Contact points and further information

The Head of Adults, Health and Well-being Department is the Council's SIRO (Senior Information Risk Owner) and therefore has responsibility and accountability at senior level.

Operational responsibility lies with Helen Parry, Information Manager.

Details about record retention periods can be obtained from the Records Management Team (site on the intranet home page).

You can also obtain further details about data protection in general from the Information Commissioner's Website – www.ico.org.uk

Appendix

In accordance with the first data protection principle, the processing of any personal data must be **justified**. One of the following conditions must be met:

1. The individual's consent (it does not have to be explicit).

2. That processing is necessary for the performance of a contract or to enter into a contract with the individual.

3. That processing is necessary in order to comply with a legal obligation.

4. That processing is necessary to protect the vital interests of the individual.

5. That the processing is necessary for the administration of justice, to carry out functions under any enactment, or to carry out functions of a public nature in the public interest.

6. That the processing is necessary for the legitimate interests of the data controller except where processing impinges upon the rights and freedom of the individual.

For sensitive personal data, one of the following conditions must **also** be met:

1. The explicit consent of the individual.

2. That the processing is necessary for the purpose of employment.

3. That the processing is necessary for the purpose of protecting the vital interests of the individual or another person where it is not possible to obtain consent.

4. That the individual has already made the information public.

5. That the processing is necessary for the purposes of legal proceedings.

6. That the processing is necessary for the purpose of administering justice.

7. That the processing is necessary for the purpose of monitoring equal opportunities.

8. That the processing is necessary for medical purposes.

There is no right to use personal information for any other purpose except in compliance with these principles. This includes

passing personal information between services or between units within services.