



Data Protection Policy

Version: Revised Policy Final

Author: Elaine McElhill, Records Management Officer

Date Approved: 11 August 2009

Status : APPROVED

Approved by: Liz Johnston, Assistant Director Administration

Review date: 6 months

Responsible Director: Catherine McFarland, Director – Corporate Services

Consultation: Assistant Director Team, Jim McKenzie, Gillian Peacocke, Trade Unions

File Ref: AVIS/Corporate Planning and Reporting/Corporate Policies/Data Protection Policy

Antrim Borough Council

Content

Data Protection Policy

	<u>Page No</u>
1.0 Introduction	2
2.0 Status of the Policy	2
3.0 Why Personal Information is Collected	2
4.0 Compliance with the 8 Principles of the Data Protection Act	2-3
5.0 Staff Awareness and Involvement	3
6.0 Contractors and Third Parties	3-4
7.0 Access to Personal Information	4
7.1 Requests by Employees	4
7.2 Requests by the Police	4
7.3 Requests by other 3 rd parties	4
7.4 Exemptions to Disclosure	4-5
8.0 Right to Prevent Processing	5
9.0 Notification to the Information Commissioner's Office	5
10.0 Conclusion	5

Data Protection Policy

1.0 Introduction

This policy sets out how Antrim Borough Council will ensure that it complies with all the provisions of the Data Protection Act 1998.

Antrim Borough Council is fully committed to protecting the privacy of all individuals including staff, contractors, service users and others, by ensuring lawful use of their personal information in accordance with the Act. The Council shall take all necessary steps to implement this policy and to ensure that all staff are fully aware of it and abide by it.

2.0 Status of the Policy

This Policy supersedes the Data Protection Policy adopted by Council in December 2001. It is a condition of employment that staff abide by the rules and policies made by the Council. This policy should be read in conjunction with the Internet and Email policy and the IT Security Policy. Any failure to follow this policy can result in disciplinary action.

3.0 Why Personal Information is Collected

In order to operate efficiently, the Council has to collect and use information about people. This may include details regarding members of the public, current, past and prospective staff members, clients, service users and suppliers. In addition, the Council may be required by law to collect and use information to comply with Government requirements.

4.0 Compliance with the 8 Principles of the Data Protection Act

The Council regards the lawful and responsible treatment of personal information as very important for successful operation and for maintaining confidence in the Council. The Council will take the following steps to comply with the 8 Principles of the Data Protection Act through appropriate management controls by:

- fully observing legal conditions regarding the lawful and fair collection and use of personal information;
- meet legal obligations to specify the purpose for which information is used and will only use it for those purposes;
- collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict limits to the length of time that information is held. Ensure that the rights of people about whom the information is held can be fully exercised under the Act;

- take appropriate technical and organizational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards.

5.0 Staff Awareness and Involvement

Staff are key to ensuring that the Council complies with the Act. The Council will ensure that

- there is an Officer employed with responsibility for ensuring that the responsibilities under Data Protection are properly discharged.
- everyone managing and handling personal information understands they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so
- anyone wanting to access their personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are regularly assessed and evaluated
- appropriate security measures are in place for managing and storing electronic and physical data. Overall computer security is the responsibility of the Assistant Director Finance. Any breaches of computer security must be referred to the Director Corporate Services.
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal information will be in compliance with approved procedures.

6.0 Contractors and Third Parties

All contractors, consultants, partners or other servants or agents of the Council who are users of personal information supplied by the Council will be required to confirm that they will abide by the requirements of the Act. The Council will require that they enter into a contract, which will oblige them to:

- ensure that they and all of their staff who have access to personal information held or processed for us or on our behalf, are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between this Council and that individual, company, partner or organisation.
- ensure that they only act on our instructions with regard to the processing of personal information we supply to them

- ensure that they have adequate security around personal information supplied to them and, in particular, will take appropriate organisational and technical steps to ensure that there is no loss, damage or destruction of such information
- allow data protection audits by the Council, of information held on its behalf (if requested)
- indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation arising out of any breach of the Act by them.

7.0 Access to Personal Information

All requests for access to personal data must be submitted in writing to the Records Management Officer, Civic Centre, 50 Stiles Way, Antrim, BT41 2UB. The Records Management Officer will handle the request in accordance with the Data Protection Subject Access Request Procedures. The request will be processed subject to the normal review process and information will be supplied within the 40 days timescale which the Act allows.

The Council under the provisions of the Act will make a charge of £10 for each written request under the Act.

7.1 Requests by Employees

Employees about whom the Council holds personal information have the right to access it, subject to condition. Employees requesting access to personal information will incur a charge of £10.00.

7.2 Requests by Police

The Police are only entitled to access personal information about individuals if it is for the following purposes:

- For the prevention or detection of crime
- The apprehension or prosecution of offenders

This is in line with the Data Protection Act 1998 Section 29 Crime and Taxation exemption.

Requests must be made on the official police issued Data Protection Form and passed to the Records Management Officer for processing.

7.3 Requests by other 3rd Parties

Requests received from other outside bodies (eg Solicitors, Suppliers, etc) will be processed in accordance with the normal review process. The Council will make a charge of £10 for each written request under the Act.

7.4 Exemptions to Disclosure

In certain circumstances it may not always be appropriate to give a data subject a copy of his/her data. Therefore Part 4 of the Act lays down circumstances where this right of access need not be given which include:

- To safeguard national security
- Where data is processed for journalism literature or art
- Where information is processed for regulatory activity ie by the Financial Services Authority
- Where the information requested is already made available to the public through any other act on payment of a fee or otherwise
- Where to disclose the data would prejudice prevention/detection of crime; apprehension/prosecution of an offender;
- If the Council is involved in negotiations with the data subject it may prejudice the negotiations
- if the request would be likely to prejudice the conduct of management forecasting or management planning
- where legal professional privilege can be claimed, the subject access provisions will not apply

8.0 Right to Prevent Processing

Section 10 of the Act gives entitlement on the part of individuals themselves to require data processing to stop, or not to start where for specified reasons it may cause substantial damage or distress to the individual or to another person.

The right to prevent processing will not be warranted when:

- consent has been given
- processing of the personal data is necessary either for the performance of a contract or when deciding to enter into a contract
- processing is necessary to comply with legal obligations
- or the processing is necessary to protect vital interest of the Council

9.0 Notification to the Information Commissioner's Office

The Act requires the Council as a Data Controller to notify our processing of personal information on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of Data Controllers, which can be found at www.ico.gov.uk.

10.0 Conclusion

Compliance with the Act is the responsibility of everyone within the Council. Any questions or concerns about the interpretation or operation of this policy should be communicated to the Director of Corporate Services.