ARMAGH CITY AND DISTRICT COUNCIL DOCUMENTED PROCEDURES QUALITY SYSTEM	
Document Number:	HR/CPP/001/Version 2
Title:	Data Protection Policy and Procedure
No. of Pages (including Appendices)	12
Version:	2
Issue Date:	
Equality screening date	2003 And again in November 2012
Amendment Version Issue Date:	
Sent out by:- Approved by:-	**Executive Committee on 06 December 2012**

AMENDMENT RECORD SHEET

Remove and destroy old pages. Insert new pages as indicated.

Revision Number	Page Number	Date Revised	Description of Revision
1	3,6,7,8,11, 12		Added sections to illustrate the Council's responsibility for the whole lifecycle of the data it processes. Removed details on I.T security as there is a separate I.T security policy

Data Protection Policy and Procedure

CONTENTS

1. POLICY SCOPE

Armagh City & District Council needs to collect and use certain types of personal information about its staff and other people it comes into contact with in order to perform its functions. This personal information must be dealt with appropriately whether it is held on paper or by electronic means and there are safeguards to ensure this under the Data Protection Act 1998.

The Council's responsibilities under the Act cover the whole lifecycle which includes;

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data;
- The disposal/destruction of personal data

The Council also has a responsibility to ensure that individuals have appropriate access, upon written request, to details regarding personal information relating to them.

- This policy should be read in conjunction with the E-Mail, Internet/Intranet, Telephone Policy, I.T Security Policy, Retention and Disposal Schedule and Access to Information Policy.

2. INTRODUCTION

In accordance with the Council's Equality Scheme the policy has been screened in order to determine whether a fuller equality analysis in the form of a policy impact assessment is required. The screening exercise resulted in a conclusion that there was no evidence to suggest that a policy impact assessment is required.

3. ACCESS TO PERSONAL DATA

The Data Protection Act 1998 aims to ensure the fair processing of data relating to employees and other people it comes into contact with (data subjects) by the Council (data controller) The Act defines 'personal data', 'data subject' 'data controller' and 'processing' as follows.

3.1 Personal data means data consisting of information, which relates to a living individual who can be identified from the information , or from that and other information in the possession of the controller.

Expressions of opinion about an individual also constitute 'personal data' but any indications of the intentions of the data controller in respect of that person do not. The 'intentions' must be the data controller's intentions, not those of a third party, for them not to be classified as personal data.

Sensitive personal data is personal data relating to the individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission or the alleged commission of an offence, or proceedings relating to such an offence.

3.2 Data subject means an individual who is the subject of personal data. Since personal data must relate to a living individual, so must the data subject be living and an individual.

3.3 Data controller is the person (Council) who determines the purposes for which and the manner in which personal data is processed. 'Processing' includes obtaining, holding and recording data.

3.4 Manual data is data, which is held on 'a relevant filing system'. A 'relevant filing system' is any collection of information relating to individuals which is structured either by reference to individuals or criteria relating to such individuals' so that such information is 'readily accessible'.

4. DATA PROTECTION PRINCIPLES

All data must be processed in accordance with the eight data protection principles.

4.1 Personal data shall be processed fairly and lawfully. In determining whether it was obtained fairly, factors such as the method by which it was obtained, whether the person who gave the information was misled or deceived as to the purposes for which it was to be held, used or disclosed will be taken into account. In the case of employees most of the basic information in the record is taken from the application form when a new recruit is taken on. In such cases individuals will be assumed to have realised that the information they were giving would be kept on record; it is therefore unlikely to be any question of them having been misled or deceived.

4.2 Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes. Data held for the purposes of unlawfully discriminating on grounds of religion, disability, race, sex, or defrauding the Inland Revenue, will be held to be in breach of this principle.

4.3 Personal data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

4.4 Personal data (not employees) e.g. where personal information is held on databases data subjects will be advised of the uses to which the data will be put and the intended recipients of the data.

4.5 Personal data shall be accurate and, where necessary, kept up to date. Data is only inaccurate if it is incorrect or misleading as to any matter of fact. Consequently, the “accuracy” of an opinion contained in personal data cannot be challenged and there is no possibility of it causing the data controller to breach this principle. Where details of criminal convictions are held, employers must be wary of keeping any record should the conviction become spent.

4.6 Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The length of time personal data is kept is linked directly to the registered purposes for keeping them.

4.7 Personal data shall be processed in accordance with the rights of the data subject under the Act.

4.8 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The Act outlines that what will be "appropriate" will depend on the harm that could have resulted from unauthorised processing, accidental loss, destruction or damage.

4.9 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. DATA COLLECTION AND DATA SHARING

5.1 The Council will:

- Observe fully, conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used or shared.
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or comply with any legal requirements.
- Make the citizen/consumer the focus of the decision when processing personal data.

6. I.T. SECURITY

The Council has a separate I.T security policy.

7. DATA SECURITY

7.1 The Council will ensure that:

- Appropriate security measures are in place to protect personal data, both automated and manual systems
- Personal data systems are accessible to authorised staff only
- Authorised staff using these systems will be advised of appropriate security procedures and the importance of their role within these procedures.

7.2 All employees are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.

- Personal information is not disclosed deliberately or accidentally;

  either orally or in writing to any unauthorised third party. Section 55 of the Data Protection Act makes it an offence to unlawfully obtain or procure personal information. The penalty is a maximum fine of £5,000.

8. DATA STORAGE AND DISPOSAL

8.1 Information and records relating to staff and other people the Council comes into contact with will be stored securely and will only be accessible to authorised staff and volunteers.

8.2 Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. The Council's retention and disposal schedule should be consulted for guidance.

9. E-MAIL, INTERNET/INTRANET, TELEPHONE POLICY, I.T SECURITY POLICY, RETENTION AND DISPOSAL SCHEDULE AND ACCESS TO INFORMATION POLICY

9.1 Employees of Armagh City and District Council should be aware of specific policies and procedures in relation to the use of email, internet/intranet and telephone communications and the Council's I.T security policy. They should also be aware of the Council's policy on the disposal of records and the processing of FOI and EIR requests.

10. SUBJECT ACCESS PROVISIONS

10.1 All data subjects have the right:

- to be informed by data controllers whether they hold personal data on them
- to be given a description of the personal data, the purpose for which the data is processed and the person(s) to whom the data may be disclosed; and
- to be supplied with this information within 40 calendar days.

If any information, which is held, is not in an intelligible form, it must be accompanied by an explanation.

10.2 The Act 1998 gives employees the right to their personal data at reasonable intervals.

10.3 In certain circumstances, the disclosure of data will involve disclosing information relating to another individual. In such cases, the employer will not be obliged to disclose the information unless the other individual has consented to the disclosure or it would be reasonable in all the circumstances to comply with such a request without such consent. This arises:

- where a data controller is involved in negotiations with the data subject, the subject access provisions will not apply if their application would prejudice the negotiations.
- any personal data which is processed by the data controller for the purpose of management forecasting or management planning done in the conduct of the business or activity of the business, will be exempt from the subject access provisions if

such access would be likely to prejudice the conduct of such business or activity

- where legal professional privilege can be claimed, the subject access provisions will not apply
- references provided by the data controller in confidence to prospective employers are exempt from the subject access provisions

10.4 Records of Grievance and Disciplinary meetings are kept for several reasons, employees should be aware that records are kept and they have a right if they so wish to inspect and receive a copy of these records on request. Spent disciplinary/grievance records will be kept on personal files.

10.5 Medical reports will only be obtained in accordance with the provisions of the Access to Personal Files and Medical Reports (NI) Order 1991 as outlined in the Council's Attendance Management Policy.

11. RIGHT TO PREVENT PROCESSING

11.1 This right entitles the data subject to prevent the data controller from beginning or continuing to process information for a specified purpose or in a specified manner. Such a request may be made on the grounds that the processing is causing or is likely to cause substantial damage or distress to the data subject or to another person and such damage or distress is or would be unwarranted.

11.2 The right to prevent processing will not, however, be available where:

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

12. ACCESS FEES

12.1 The Council may charge a fee of £10 for subject access requests.

13. PROCEDURE FOR EMPLOYEES ACCESSING THEIR PERSONAL DATA

13.1 The Act 1998 gives employees the right to have access to their personal data at reasonable intervals.

13.2 All employees will have access to their personal file by appointment outside core hours in the presence of a member from the HR Department. Employees are required to inform HR if they have any change in circumstances so that their personal file and records can be updated – i.e change of address.

13.3 If an employee disagrees with the personal data held on record, they should inform a member of the HR department or their line manager, and may, if the matter has not been resolved, raise the matter under the Council's grievance procedure.

13.4 The Council must retain personal records for a period of seven years after an employee leaves Council employment.

13.5 HR will undertake annual reviews of personal data held to ensure that there is still a need to keep the data

14. DATA ACCESS AND ACCURACY

14.1 All Data Subjects have the right to access the information Armagh City & District Council holds about them. The Council will also take reasonable steps to ensure that the information is kept up to date by asking data subjects whether there have been any changes.

14.2 In addition, the Council will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection,
- Chief Officers are responsible – for communications and issues relating to information security, the Data Protection Act, and other related legislation within their department.
- All activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information security and compliance with the Act;
- All contracts and service level agreements between the Council and external third parties, where personal data is processed, make reference to the Act as appropriate.
- All staff acting on the Council's behalf understand their responsibilities regarding information security under the Act, and that they receive the appropriate training/instruction and supervision so that they carry out these duties effectively and consistently and are given access to personal information that is appropriate to the duties they undertake;
- All third parties acting on the Council's behalf are given access to personal information that is appropriate to the duties they undertake and no more;
- Any requests for access to personal data are handled courteously, promptly and appropriately, ensuring that either the data subject or his/her authorised representative has a legitimate right to access under the Act, that the request is valid and that information provided is clear and unambiguous.
- It will regularly review and audit the way it holds, manages and uses personal information

15. REVIEW

15.1 The policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.