ANGUS COUNCIL

ITEM No. 11

POLICY AND RESOURCES COMMITTEE - 23 OCTOBER 2001

DATA PROTECTION ACT 1998

REPORT BY DIRECTOR OF LAW AND ADMINISTRATION

ABSTRACT
This Report advises Committee of the requirements placed upon the Council by the Data Protection Act 1998 and of the measures taken by the Council to implement the Act. This Report also makes recommendations with respect to the approval of a Council-wide data protection policy and with regard to charging for subject access requests under the Act.

1. RECOMMENDATION

The Committee is requested:-

(a) to note the work undertaken by the Council to implement the Data Protection Act;

(b) to approve the Data Protection Policy attached as Appendix A; and

(c) to approve the recommendation contained in this Report that no fee be charged for subject access requests made under the Act.

2. BACKGROUND

The Data Protection Act 1984 was introduced with a view to protecting the individual from possible misuse of information stored on computer. The 1984 Act has now been replaced by the Data Protection Act 1998, which is much wider in its scope, in that it now includes information contained in paper files in its definition of "data". Although passed in 1998, the Act has been implemented in a series of stages. The most significant implementation date for the Council will be 24 October 2001.

Broadly, the Act has two main aims. It gives data subjects (ie individuals about whom information is held) certain rights, including the right to access and receive a copy of the information held about them. The 1998 Act also requires data controllers (ie bodies who hold information about individuals, such as the Council) to follow the eight data protection principles.

The Information Commissioner has wide enforcement powers in relation to the Act and can serve Enforcement Notices on data controllers and fine them. Breaching the Act can also, in certain circumstances, be a criminal offence.

3. THE KEY POINTS OF THE 1998 ACT

3.1 Notification

Under the Act, every organisation which uses or processes information relating to a living individual (this is known as "personal data") must formally register this fact with the Information Commissioner at regular intervals. This is called "notification". The notification to the Commissioner must include details of the type of information held, the source of the information, the purposes for which the information is being held and to whom or what the information is disclosed or released.

The notification is currently kept up to date by the Director of Information Technology. The Information Commissioner has introduced a single notification document to be used by Scottish Local Authorities which should make the notification process simpler in the future.

3.2 Data Protection Principles

The data protection principles set out in the Act operate as a mandatory code for processing personal data. (The definition of "processing" is very wide under the Act and covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.)

The eight principles can be summarised as follows:-

(i) personal data shall be processed fairly and lawfully;

(ii) personal data obtained for one purpose shall not be used in a manner which is incompatible with that original purpose;

(iii) personal data should be adequate, relevant and not excessive;

(iv) personal data should be accurate and, where necessary, kept up to date;

(v) personal data shall not be kept for longer than is necessary;

(vi) personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;

(vii) 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;

(viii) 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.

3.3 Subject to certain exceptions, members of the public are entitled to see any personal information held about themselves, to receive a copy of such information, to have it corrected where necessary and, in certain circumstances, to claim compensation for a failure to comply with the Act.

The Act specifically states that all subject access requests must be made in writing. Generally speaking, a subject access request must be complied with within 40 days of receipt.

3.4 Subject Access Requests by Elected Members Etc on Behalf of Constituents

In terms of the Act, Elected Members, MPs, MSPs and MEPs do not have a right to have unrestricted access to personal data held by the Council or, indeed, to personal data held about one of their constituents, even where the constituent has asked him or her to look into a particular matter on his or her behalf. As a result, a subject access request made by an elected representative must be made in writing and must be accompanied by written authorisation from their constituent. Appropriate forms are available and a brief training session has been arranged for members, MPs, MEPs and MSPs.

3.5 Subject Access Requests by Members or Employees

As with elected representatives, Council employees have no automatic or unrestricted right of access to personal data held by the Council, either about themselves or about any other person. Internal subject access requests made by an Elected Member or employee in respect of their own personnel or payroll records should be made directly to the nominated departmental contact. Access requests to any other type of personal information (for example Council Tax records) must be made as a private individual through the formal subject access procedure.

4. DATA PROTECTION WORKING GROUP

A working party, chaired by the Head of Legal Services and comprising representatives of every Department, has been carrying out work to ensure that the Council is prepared to discharge its responsibilities under the Act. Amongst its principal actions have been:-

(i) an audit of current departmental practice and file and record management against the principles set out in the Act;

(ii) the development of publicity material relating to subject access. The Group has produced two sets of information leaflets on subject access - a summary and a detailed explanation of their rights for members of the public and a summary for all employees, as well as detailed guidance for those involved in dealing with subject access requests. Copies of these leaflets will be available in the Members' Lounge;

(iii) the development of a detailed procedure note to be used by all employees (except Social Work employees - see 5 below), who will be required to facilitate a subject access request. This procedure note explains how to deal with such things as the exemptions contained in the Act, third party information and the timescales involved. It also deals with such matters as security of data, for example ensuring that the person making the application is in fact the subject of the information, or has been authorised by the subject of the information to make the request;

(iv) the identification of training/briefing requirements for employees. As all departments are represented on the group, each has a source of in-house expertise on data protection. Additionally, the audit of current practice requires departments to review their approaches to file management and record management. However, there remains a need to ensure that those employees who have responsibilities for data are aware of the implications of the Act. It is therefore intended that a briefing session on the principal issues arising from the Act will be held for two senior members of each Department in mid-October. That session will also be used to identify whether, and if so what, arrangements are needed to cascade the material throughout departments.

Members, MPs, MEPs and MSPs will also be offered briefing on the Act.

(v) the preparation of a draft data protection policy (see Appendix A). This draft policy was considered and approved by the Chief Officers Management Team on 24 September 2001 and it is recommended for approval by Committee.

In addition to the work of this group, the Director of Information Technology has developed the Council's IT and Information Security Policy, which addresses a number of areas relating to maintenance of data confidentiality and the proper handling of information as required by the Act.

5. ROLES AND RESPONSIBILITIES

It is the responsibility of the Director of Law and Administration to provide legal advice on the Act and to co-ordinate the work of the Council's Data Protection Act Working Group for as long as the Group continues to meet. She will also be responsible for keeping a central register of any subject access requests received by the Council and for monitoring the manner and timescales in which subject access requests are dealt with. (It should be noted, however, that all subject access requests made in respect of Social Work records will continue to be monitored by the Director of Social Work. Social Work records have, along with certain other records, been accessible since the introduction of the Access to Personal Files Act 1987, which has now been subsumed by the Data Protection Act 1989. Consequently, Social Work already have systems in place for dealing with subject access requests.

The Director of Information Technology is currently the Council's Data Protection Officer and is, as mentioned earlier, responsible for the Council's notification to the Information Commissioner. Whether it would be appropriate for this post to be transferred to the Director of Law and Administration, will be the subject of discussion between both Directors in due course.

Directors will be responsible for all aspects of compliance with the Act within their department, ensuring that adequate procedures are in place for records management, back-up and storage management and destruction, where appropriate, of personal data. Each department will appoint a data protection representative to co-ordinate compliance with the Act, including security, subject access requests and employee awareness.

Further clarification of roles and responsibilities is given in Appendix A.

6. CHARGING FOR SUBJECT ACCESS REQUESTS

One issue relating to subject access requires to be resolved. The Act allows the Council to make a charge of a maximum of £10.00 (a maximum of £50.00 for certain Education records) for dealing with a subject access request. This figure will not cover the cost of making the search for the data, which is likely to be considerably higher. It is also unlikely to act as a deterrent to frivolous information requests. At present the Council's policy is not to charge for subject access requests made under the Data Protection Act 1984. The general approach by local authorities throughout Scotland is mixed, with some choosing to waive the charge, some making a charge and others only charging in specific circumstances.

It is proposed that the Council makes no charge for the service meantime but reviews this decision after a year. This recommendation was also considered and approved by the Chief Officers Management Team on 24 September 2001 and it is recommended for approval by the Committee.

The low figure chargeable is unlikely to act as a deterrent for frivolous subject access requests and, it should be noted, where an individual makes repeated and/or vexatious subject access requests, the Council is entitled to refuse to deal with the request.

7. FINANCIAL IMPLICATIONS

It is impossible to calculate the financial implications of the Data Protection Act 1998 with any certainty, given that the cost will depend on the number of subject access requests made under the Act. Requests for subject access requests made under the Data Protection Act 1984 were few and far between, although the publicity which the Information Commissioner is planning for the 1998 Act may result in a surge of subject access requests being made.

It should also be noted that the number of requests for access to Social Work records has been steadily increasing over the years.

There may also be other cost implications to departments, particularly with regard to ensuring that all of the information they hold conforms with the data protection principles.

Any costs incurred as a result of the 1998 Act will require to be covered by existing budgets.

8. HUMAN RIGHTS IMPLICATIONS

There are no human rights implications arising as a result of this Report. However, it should be noted that any breach of the Data Protection Act which affects the security of personal information could result in the Council breaching both Article 8 of the European Convention of Human Rights, (the right to respect for private and family life, home and correspondence), as well as the seventh data protection principle. It is therefore important for the Council to have robust policies in place to ensure that such a breach does not occur.

9. CONSULTATION

The Chief Executive and all Directors have been consulted in the preparation of this Report.

10. CONCLUSION

The Data Protection Act 1998 is an important piece of legislation, which allows wider public access to personal information and which will affect the way in which Angus Council, as a data controller, manages the personal information which it holds.

CATHERINE A COULL
Director of Law and Administration

NOTE: No background papers as defined by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information) were relied on to a material extent in preparing the above Report.

g:\wp\cttee\rp2001\1214.rtf

DATA PROTECTION ACT 1998

STATEMENT OF COUNCIL POLICY

1. Introduction

The Data Protection Act 1998 sets out rules for the processing of personal information held in paper form and/or in computer files. The Act establishes a series of eight principles of good information handling, which are set out below. The Council undertakes to comply with these principles in all matters relating to the processing of personal information.

The eight data protection principles can be summarised as follows:

1. Personal data shall be processed fairly and lawfully.

2. Personal data obtained for one purpose shall not be used in any way which is incompatible with that purpose.

3. Personal data should be adequate, relevant and not excessive.

4. Personal data should be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. 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.

8. 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.

2. Scope

This Policy is applicable to all personal data held by Angus Council within the definition contained in the Data Protection Act 1998.

This Policy applies to all employees and elected members of Angus Council and any contractor (or agent) performing work for or on behalf of Angus Council.

3. Roles and Responsibilities

The Director of Information Technology is the appointed Data Protection Officer for the Council. As the Data Protection Officer, he is responsible for the Council's notification to the Information Commissioner and for ensuring that all Departments of the Council are able to comply with the Act.

The Director of Law and Administration is responsible for providing legal advice on the Act and for co-ordinating the work of the Council's Data Protection Working Group. She is also responsible for monitoring the manner and timescales in which subject access requests are dealt with, although the Director of Social Work is responsible for monitoring such requests for social work records.

Directors are responsible for all aspects of compliance, ensuring that adequate procedures are in place for records management, back-up and storage management and destruction, when appropriate, of personal data.

Each department will appoint a data protection representative to co-ordinate compliance with the Act, including notification, security, data subject access requests, data matching and employee awareness.

This policy will be reviewed as necessary by the Data Protection Officer and by the Director of Law and Administration to ensure compliance with legislation and fulfilment of Council requirements.

4. Compliance

All personal data will be held in compliance with the Data Protection Act 1998.

5. Notification

The Council will ensure that its notification with the Information Commissioner is regularly reviewed and updated where appropriate.

6. Security

All departments must ensure that they have in place systems and procedures to protect the confidentiality and security of data, having regard to the nature and sensitivity of the data held.

All employees must ensure that the data they hold is treated confidentially and must adhere to corporate policies and individual departmental guidance in this respect.

7. Third Party Compliance

Contracts for the processing of information by a third party on behalf of the Council must include confidentiality and security clauses. The Council must be satisfied that the information security measures adopted by any contractor (or agent) directly or indirectly in the employment of the Council comply with the terms of the Act.

8. Employee Responsibilities

Employees with access to personal information must be familiar with and adhere to the requirements of the Data Protection Act 1998 and the eight data protection principles laid down in the Act.

Employees with responsibilities for handling personal data will be given awareness, induction and update training on the requirements of the Act as appropriate.

Employees must follow any corporate or departmental guidance on adhering to the Act.

Failure to adhere to this policy and any related guidance will be regarded as a disciplinary offence.