PORTFOLIO: POLICY & STRATEGY

CABINET - 8 JULY 2002

COMPLIANCE WITH THE DATA PROTECTION ACT 1998

1. INTRODUCTION

1.1 The purpose of this report is to inform Members of a review undertaken by the District Auditor of the Council's compliance with the requirements of the Data Protection Act 1998 and to seek approval for the approach to be adopted in response to the recommendations made.

1.2 The review was carried out at the end of 2001 and reported on the Councils preparedness for a number of requirements that came into force in October of that year.

1.3 The objectives of the review were to:

- Identify the management arrangements in place to achieve compliance with the legislation
- Review the plans made by the Council to prepare for notification of the purposes under which data is processed
- Ensure that all actions necessary to deal with transition to the requirements of the new Act had been identified
- Evaluate the robustness of the Council's data protection management system
- Evaluate, where possible, the robustness of the Council's policies for ensuring accuracy of data
- Review the Council's ability to comply with the data subject access request within 40 days
- Review the Council's procedures and protocols for ensuring legal external transfer of data
- Ensure that the Council's information security policy addressed the requirements of the Data Protection Act
- Agree a series of actions to ensure compliance

1.4 The District Auditor reached the conclusion that the Council was slightly above the average for Local Authorities in its level of preparedness for compliance with the new Act but was below the overall target that it had set for evaluation purposes.

1.5 The report recognised that responsibility for Data Protection lies with an experienced Data Protection Officer (DPO) but that Data Protection is only one of many responsibilities of the present postholder. It also noted that the approach adopted by the Council reflects the nature of the organisation i.e. a public body undertaking primarily statutory functions, the type of data held, the history of good data management and the historically very low public interest in the data held.

1.6 The report included an agreed action plan covering all issues identified as a result of the report. The action plan is attached at Appendix 1. A further column has been added to the action plan which identifies what progress has been made since the report was issued.

2. KEY ISSUES / PROGRESS

2.1 Progress has been achieved against many of the action points since the report was received. The following section seeks to focus on the key issues identified in the report and the proposed courses of action to deal with the matters.

2.2 The report identified that responsibility for Data Protection should lie with a Chief Officer with a corporate role who currently has it high on the agenda. The DPO should be regularly reporting upwards.

Action: Responsibility currently lies with the Director of Resources. Weekly progress meetings are held between the DPO and the Assistant Director Resources. Progress against the action plan is discussed. Matters of consequence are then reported to the Director of Resources as necessary. It is not proposed to change this arrangement.

2.3 Because of the increased awareness generally of the rights of individuals (Human Rights Act, Freedom of Information Act, Data Protection Act) it was recommended that information management should be a regular agenda item for CMT.

Action: Reports have historically been brought to CMT to seek approval in response to specific issues. A number of officers have responsibility for corporate information management (ICT, Legal, DPO). A joint annual report could be tabled to CMT to include ICT security, Data Protection and Freedom of Information.

2.4 Responsibility for implementing and co-ordinating Data Protection compliance across the Council lies with the DPO. The report recommends that consideration should be given to the creation of an informal group of directorate representatives with data protection responsibilities.

Action: *A similar team could be created to that currently in place for the implementation of the Freedom of Information Act (FOIA). Alternatively the terms of reference of the FOIA group could be extended to include responsibility for Data Protection as well. Either approach would have the benefit of establishing quasi directorate experts.*

As the longer term responsibility for managing FOIA compliance has yet to be determined It is proposed that the current arrangements should remain but that the possibility of extending the terms of reference of the FOIA group to include Data Protection be explored once the impact of the FOIA is known.

2.5 The report recognised that the Council has a Data Protection policy in place. This has not been formally approved by either CMT or Cabinet.

Action: The Data Protection Policy is attached at Appendix 2. Approval is sought for its formal adoption.

2.6 The introduction of the 1998 Act extended the requirement for Data Protection compliance to some manual as well as automated data. Organisations are required to maintain records of what qualifying data exists, ensure that all purposes for processing have been notified to the Information Commissioner, and that the way in which the Council holds personal data complies with the data protection principles. Currently central records of data activity are maintained manually. The audit identified that with the scope and complexity of requirements now in place the DPO would benefit from the introduction of a computerised data protection management system.

Action: An Access database has recently been acquired. It will act as a central register of all personal data held and will assist in the management of the Council's Data Protection responsibilities. Information relating to all of the Councils electronically held / processed data has been entered onto the database. This will shortly be updated with information relating to all manually held personal data.

2.7 In addition to the issues identified in the report it is also considered appropriate that a change to the Council's charging policy for Data Subject Access Requests should also be made at this time. The current maximum prescribed fee chargeable under the Act for such requests is £10.00. Since the introduction of the Data Protection Act in 1984 Council policy for charging for Subject Access Requests has been to allow a first request free of charge and for subsequent requests to be charged the maximum fee of £10.00.

2.8 Over the past few years the annual number of formal individual requests for information has not exceeded more than 5 in any one year. It is not believed during this time that any requests made have necessitated the £10.00 fee being charged. With the prospect of a heightened public awareness in respect of individuals rights (Human

Rights Act, Data Protection Act, Freedom of Information Act) it is possible that the quantity of requests submitted for information could start to grow. Whilst the Council will clearly wish to continue to be open about the information that it holds there is a danger that in not charging for a first request there is no deterrent to the submission of vexatious requests.

2.9 It is therefore considered that a change in the current charging policy, to introduce a fee of £10.00 for each and every request for information under the Data Protection Act, would be a sensible measure to take.

2.10 Requests for images by individuals from the new town centre CCTV system also fall under the requirements of the Data Protection Act. Any requests for CCTV information will be satisfied by providing a paper copy of the image. If individuals insist on requiring an electronic copy in either DVD / CD or videotape format the cost of satisfying such requests could be considerable. Images of 3rd parties would have to be erased. The Council would have to engage the services of a specialist editing house to undertake this technical work.

2.11 It is therefore proposed that such requests be charged for at actual cost, to be determined on a case by case basis.

3. FINANCIAL IMPLICATIONS

3.1 The cost of the computerised data protection management system was £500 and was funded from within existing budgets in 2001/02.

3.2 Failure to introduce a fee could encourage high levels of inappropriate subject access requests to view images recorded by the Council's Town Centre CCTV system. This would result in a significant use of resources.

3.3 The introduction of a £10.00 fee is very unlikely to generate significant levels of income in the future.

4. ENVIRONMENTAL IMPLICATIONS

4.1 None

5. CRIME AND DISORDER IMPLICATIONS

5.1 None

6. CONCLUSIONS

6.1 The District Auditor reached the conclusion that the Council was slightly above the average for Local Authorities in its level of preparedness for compliance with the new Act but was below the overall target that it had set for evaluation purposes.

6.2 Since the audit review further work has been undertaken to ensure that the Council deals with the requirements of the Data Protection Act appropriately. Whilst there remain a number of areas that still require attention (see action plan) it is considered that the arrangements now in place or planned for the future will ensure a satisfactory level of compliance with the requirements of the Act.

7. RECOMMENDATIONS

It is recommended that Members approve:

7.1 The current reporting arrangements and responsibilities for Data Protection as set out in 2.2 – 2.4.

7.2 The Data Protection Policy at Appendix 2.

7.3 The introduction of a £10.00 fee for each and every subject access request under the Data Protection Act.

7.4 The charging of the actual cost of requests for images of CCTV footage where individuals insist on requiring an electronic copy in either DVD / CD or videotape format.

And that Members note:

7.5 The progress made to date against the action plan included at Appendix 1.

Further Information:

Geoff Bettle
Principal Auditor & Data Protection Officer
Ext 5820
geoff.bettle at NFDC

Background Papers:

District Audit Report - Compliance with the Data Protection Act 1998
Data Protection Act 1998

Action Plan

APPENDIX 1

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
1	1.2	Identify/appoint a Chief Officer to lead on Data Protection	●	○			23/10/01	Recommendation in report
2	1.3	Ensure Data Protection Officer is trained and has resources	●	○	GB		Ongoing	Ongoing
3	1.4	Information Management on Management Team agenda	●	○			23/10/01	Recommendation in report
4	1.5	Project Team of all Depts with Chief Officer as sponsor	●	○	GB / CM	To be considered	April 2002	Recommendation in report
5	1.6	Data Protection Policy in place, covers 1998 Act	●	○		Policy in place – To be reported to CMT	April 2002	For approval in report
6	2.1	Timetable of expiry of current registrations, and way forward	●	●			31/08/01	Completed
7	2.2	Review accuracy of existing registrations	●	●			31/08/01	Completed
8	2.3	Reduce register entries to one Notification	●	●			31/08/01	Completed
9	2.4	Audit manual systems	●	○	GB	Underway	Dec 2001	Completed – to be entered on data base
10	2.5	Decision on Security Policy statement for Notification	●	○	ICT	ICT currently working towards BS7799	Ongoing	Benefits of formal adoption of BS7799 being

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
								considered by ICT
11	2.6	Purposes for Notification are identified	●	●			31/08/01	Completed
12	3.2	Action Plan for Transition	●	○	GB		April 2002	July 2002
13	3.3	Identify 'new processing' (i.e. from 24.10.1998)	●	○	GB	Part of review of manual systems	Dec 2001	July 2002
14	3.4	Project control of the data audit	●	○	GB	Part of review of manual systems	Dec 2001	Database purchased, automated systems entered
15	3.5	Schedule of personal data, identifies Schedules 2 & 3 data	●	○	GB		April 2002	Sept 2002
16	3.6	Identify data exempt from transition rules	●	○		N/A Working on principle that no data is exempt from provisions of the Act		N/A
17	3.7	Policy on consent, identify forms containing implicit consent	●	○	GB		Ongoing	Ongoing
18	4.1	Ensure all purposes can be linked to all relevant data sets	●	○	GB	Completing as part of manual / automated data review	April 2002	July 2002
19	4.2	Instructions given to staff dealing with sensitive personal data	●	○	GB		April 2002	July 2002

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
20	4.4	DPO informed of proposed new or changed systems	●	○	GB / ICT		April 2002	Completed
21	4.5	Monitoring system should identify disclosures of data	○	○	GB	Part of ongoing training of staff	Ongoing	Ongoing
22	4.6	System should identify changes of data or its use	○	○		Unlikely that resources available to address setting up of centralised system		Responsibility should lie with system owners
23	4.9	Justification for data classification and Publication Policy	●	○		Low priority, may depend on approach to FOI Act		To be considered as part of adoption of BS7799 as this required a data classification system
24	5.1	Procedures on initial data accuracy and data entry	●	○		Unlikely to produce corporate procedures, services exercise their own controls		Responsibility of system owners
25	5.2	Instructions to staff on data accuracy	●	○	GB	Covered through on-going staff training	Ongoing	Ongoing
26	5.4	Data change checking procedures	●	○		Responsibility of service managers to apply procedures to ensure data accuracy		Responsibility of system owners

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
27	5.5	Identified which data is checked by data subjects, 3rd parties	●	○		Key systems subject to annual checks by data subjects e.g. HB, C Tax, Rents etc		Ongoing
28	5.6	Timetable of periodic checks on personal data	○	○		Services advised on ad-hoc basis, included as part of staff training, not seen as priority for central monitoring		Database will assist review process
29	5.7	Timetable for retention of data on live and in store	●	○	GB	Long term ideal but low priority		Dec 2002 - with FOI Act
30	6.1	Raise profile of DPO with front-line staff	●	○	GB/ ICT	To be included in induction programme, Publicity to be issued shortly	Jan 2002	Publicity issued Jan 2002 / ongoing
31	6.2	Ensure staff aware of 40 day rule	●	○	GB	Achieved through ongoing training / awareness	Ongoing	Ongoing
32	6.3	Data subject access procedure in place, forms available	●	●			31/08/01	Completed
33	6.4	Data subject access procedure tested	●	●			23/04/01	Completed
34	6.5	Guidance to DPO on 3rd party identifiers and age of minority	●	○	GB / Legal	Low priority	April 2003	April 2003
35	6.7	Identify all data subject to automated decision making	●	○	GB		July 2002	Completed
36	7.1	Vetting procedure for overseas transfer of data	○	○			July 2002	July 2002

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
37	7.2	Web publishing policy in place	○	○	GB	Check with Public Relations on the publication of personal data	July 2002	COP on Web-site DP compliance recently issued by Info Commissioner. ICT reviewing to ensure compliance
38	7.3	E-mail policy and guidance to staff	●	○		Exists		Completed
39	7.4	DPO involvement in protocols.	○	○	GB	Applies to CCTV & Crime Prevention work, DPO involved on ongoing basis	Ongoing	Ongoing
40	7.5	Procedure for assuring compliance of external suppliers	●	○	GB	Include as part of procurement strategy	April 2003	April 2003
41	8.1	Review staff conditions of service	●	○	GB/ Personnel		July 2002	Completed Included in ICT Security Policy & Disciplinary rules
42	8.2	Staff awareness and training programme	●	○	GB	Induction / staff awareness	Ongoing	Ongoing
43	8.3	Review of controls over notified data part of audit programme	●	○	GB	Register being set up, scope for reviewing data dependant upon	Register (Jan 2002)	Checklist produced for integration in all

Action point	Section ref	Action	Started	Completed As at 1.1.02	Responsibility	Comments	End date	Current Status
						resources		Audit reviews of systems using personal data
44	8.4	Address security over manual files	●	○	GB	Covered as part of review of manual systems	Jan 2002	July 2002

APPENDIX 2

NEW FOREST DISTRICT COUNCIL DATA PROTECTION POLICY

New Forest District Council needs to collect and use certain types of information about people in order to effectively carry out its day to day operations, many of which are statutory requirements.

Information collected includes, among others, current, past and prospective;

- Employees
- Taxpayers
- Benefit / Grant claimants
- Housing tenants
- Suppliers
- Customers / Users of services

Personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or other material.

The lawful and correct treatment of personal information is regarded as very important to the successful operation of all Council business and to maintaining confidence with all individuals and organisations with whom the Council has contact.

The Council fully endorses and adheres to the Principles of data protection. Specifically the Principles require that personal information:

- Shall be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met;

- Shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes;

- Shall be adequate, relevant and not excessive in relation to the purpose for which it is processed;

- Shall be accurate and where necessary kept up to date;

- Shall not be kept for longer than is necessary for that purpose;

- Shall be processed in accordance with the rights of data subjects under the Act;

- Shall have appropriate technical and organisational measures in place to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, 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.

New Forest District Council will therefore, through appropriate management, strict application of criteria and controls:

- Fully observe the conditions regarding fair collection and use of information;

- Meet its legal obligations to specify the purposes for which information is used;

- Collect and process appropriate 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 checks to determine the length of time information is held;

- Ensure that the rights of people about whom information is held are able to be fully exercised under the Act. (These include the right to be informed that processing is being undertaken, the right of access to one's own personal information, the right to prevent processing in certain circumstances and the right to correctly rectify, block or erase information which is regarded as wrong information);

- Take appropriate technical and organisational measures to safeguard personal information;

- Ensure that personal information is not transferred abroad without suitable safeguards.

New Forest District Council will ensure that there is someone with specific responsibility for data protection in the organisation. (Currently the nominated person is Geoff Bettle, Principal Auditor and Data Protection Co-ordinator 023 80285820 or e-mail Geoff Bettle at NFDC).

All employees managing and handling personal information will be appropriately trained and supervised. All enquiries about the handling of personal information will be dealt with promptly and courteously.

A regular review will be undertaken of the way in which personal information is managed.

GJB
24/05/02