THANET DISTRICT COUNCIL

DATA PROTECTION ACT 1998

POLICY & PROCEDURES

Version Control

Version 1 – 13 April 2011
Version 2 – 21 April 2011
Version 3 - 4 May 2011

Gary Cordes
Legal Services Manager
Corporate & Regulatory Services
Thanet District Council
PO Box 9
Cecil Street
Margate CT9 1XZ

Contents

1. SUMMARY

Thanet District Council must ensure all personal information is processed in accordance with the Data Protection Act 1998. The policy explains how Members and Officers are expected to comply with Act. The Council must comply with this policy to the ensure Data Protection Act is not breached. Any breach of the Act has serious consequences for the organisation and its customers.

2. INTRODUCTION

The Data Protection Act 1998 (The Act) aims to protect all personal data which is collected, processed, stored and disposed of by an organisation. Personal data is information about a living, identifiable person. The Act applies to data in paper and electronic format.

The Act supports Article 8 of the Human Rights Act, which gives an individual 'the right to respect for his private and family life, his home and his correspondence.'

Everyone must respect confidentiality in the working environment. We must take care in disclosing information to others – within our own teams and sections, to other services within the Council and externally to other organisations.

The Information Commissioner's office (ICO) is responsible for regulating and enforcing the Act. The ICO is an independent authority which has legal powers to ensure organisations comply with the Act. Fines of up to £500,000 can be issued to organisations which breach Data Protection requirements.

3. SCOPE

This policy applies to elected members and all employees working for the Council, (including consultants, volunteers and contractors) and external data processors instructed by the Council who are handling data on behalf of the Council. Everyone handling personal data should understand and comply with the principles of the Data Protection Act.

4. POLICY STATEMENT

It is the responsibility of all Tier 2 Managers to ensure that their staff are aware of and adhere to this and all other Data Protection Act (DPA) policies and procedures and have received relevant Ivysoft training. Tier 2 Managers must ensure that all new staff complete the latest induction training that includes a section on DPA. All new DPA requests, data breaches or suspected data breaches must be referred immediately to the Deputy Data Protection Officer in Legal Services. Tier 2 Managers shall arrange the destruction of personal data as soon as possible after minimum retention periods have expired. Contact the Deputy Data Protection Officer in Legal Services if you are uncertain about any aspect of the Council's DPA policies and procedures or the DPA generally.

The Council is committed to ensuring compliance with the Act and will:

- Respect the rights of each individual
- Be open and honest about the personal data it holds

- Provide training and support to those handling personal data in the course of their duties
- Notify the ICO that it processes personal data. This is a statutory requirement and notification must be submitted annually. Notification must be kept up to date. Any changes to the use of personal data being updated within 28 days. The Democratic Services Manager maintains the annual notification with the ICO on behalf of the DPO.
- Inform the ICO of breaches of the Act (where required)

5. WHAT IS PERSONAL DATA?

Any personal information that is processed, is readily accessible and relates either directly or indirectly to a living, identifiable person who can be identified from the data or from data and other information which is in the possession of, or is likely to come into the possession of the Data Controller.

Personal data includes an expression of opinion about the individual and any indication of the intentions of the Data Controller, or any other person in respect of the individual.

6. OTHER DEFINITIONS

Data Controller — All users of personal information are Data Controllers (individuals and the Council as a whole).

Data Protection Officer — The responsible person within the Council for all matters connected with the Data Protection Act. The Data Protection Officer is also responsible for notifying the Information Commissioner of personal data held and processed by Thanet District Council.

Data Subject — The individual to whom the information relates.

Disclosure Recipient — Organisations or individuals to whom the data can be given or disclosed.

Personal Data: — Data relating to a living individual who can be identified from that data (or from that data combined with other information in the possession of the Data Controller).

Processing — Obtaining, recording, holding or carrying out any set of operations on the information or data, including organising, adapting, altering, retrieving, consulting, using, transmitting, disseminating, making available, aligning, combining, blocking, erasing or destroying.

Sensitive Personal Data: — The Act makes a distinction between ***Personal Data*** and ***Sensitive Personal Data.*** Sensitive Personal Data includes:

- Racial or Ethnic Origin
- Political Opinions or Persuasion
- Trade Union Membership or Affiliation
- Physical or Mental Health or Condition
- Sexual Life
- Commissioned or Alleged Commission of Offences

- Any proceedings for any offence, committed or alleged, including any sentencing decisions made by the Court.

Subject Access Anyone who thinks that the Council is holding data about him or her is entitled to receive a copy of the information or to be told that no data is held about them. Applicants must identify themselves and specify which data they wish to see. Applications should in the first instance be made in writing to the Data Protection Officer. The Council is under a legal obligation to comply with a subject access request (SAR) submitted with the required fee (currently £10) within 40 days of its receipt.

Source Where the data entered into a computer system or filing system originates from.

7. THE RIGHTS OF THE DATA SUBJECT

The Act provides individuals with a number of rights relating to their personal data:

7.1 **Accessing Information:** This allows an individual to find out what personal data the Council holds about them. For further information please refer to the Subject Access Request (SARS) Policy & Procedures (Annex 1)

7.2 **Correcting Information:** An individual has the right to correct, block, remove or destroy personal details which are factually inaccurate. This may be agreed with the Council's Data Controller. In some cases the Data Subject may need to refer to the ICO, or apply for a court order to make these changes. In all cases the Council must keep the original data as a record of its actions, even is this has been corrected. A copy of the amended record should be sent to the Data Subject for their records.

7.3 **Preventing Processing of Information:** The Council can be asked not to process data which may cause substantial or unwarranted damage or distress to the individual. The Council is not always bound to act on the request.

7.4 **Preventing Unsolicited Marketing:** The Council is required not to process data about an individual for direct marketing purposes, when the individual has specified he/she does not want direct marketing, e.g. sending unsolicited mail.

7.5 **Preventing Automated Decision Making:** An individual can object to decisions being made by automatic means, i.e. where there is no human involvement.

7.6 **Claiming Compensation:** An individual can claim compensation from the Council through the courts for damage and, in some cases, distress, caused by any breach of the Act.

7.7 **Requesting a Review of Data Processing:** An individual can ask the ICO to investigate and assess whether the Council has breached the Act.

8. THE 8 DATA PROTECTION PRINCIPLES

The Act states that anyone who processes personal data must comply with 8 principles which ensure that personal information is:

8.1 Fairly and lawfully processed

8.2 Processed for limited purposes

8.3 Adequate, relevant and not excessive

8.4 Accurate and up to date

8.5 Not kept for longer than is necessary

8.6 Processed in line with your rights

8.7 Secure

8.8 Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

9. ROLES AND RESPONSIBILITIES

Thanet District Council has appointed the Corporate and Regulatory Services Manager as the Data Protection Officer with responsibility for ensuring all members of staff handling personal data are compliant with the Act. The Legal Services Manager will be Deputy Data Protection Officer.

Anyone representing the Council has a duty to protect the information it holds. Access to personal data must be on a strict need to know basis. Personal data must not be discussed or disclosed without appropriate authorisation.

Any member of staff who knowingly or recklessly breaches the Council's Data Protection Policy and Procedures may be subject to internal disciplinary procedure. This is in addition to the civil and criminal remedies available to the Information Commissioner under the Act.

.Authorisation from a Tier 2 Manager must be obtained before an employee is permitted to use a privately owned computer to process personal data belonging to the Council or to take personal data out of the Council's offices for processing on a computer owned by the Council or for any other purpose.

10. ELECTED MEMBERS

Elected members may have access to, and process personal data, in the same way as employees, and must comply with the 8 Data Protection Principles. Since data held on council systems may be used by elected members in their other roles the data controller may be the elected member or the council individually, jointly or on behalf of others.

Notification should be arranged as follows:

- When acting on behalf of the council, councillors can rely on the Council's notification.
- When acting on their own behalf (e.g. when dealing with complaints made my local residents) councillors must notify the ICO in their own right.
- When campaigning within their own political party councillors may rely on the notification made by their party.

For ease of retrieval elected members should store council data separately from data relating to their other work (e.g. ward and political party work).

11. PRIVACY NOTICE (FORMERLY FAIR PROCESSING)

All Thanet District Council forms and notices which expect an individual (data subject) to provide personal information require a mandatory privacy notice. For this purpose, managers must ensure that a suitably worded 'privacy notice' is attached to all forms on which personal data is being collected. The privacy notice will explain why the information is being collected and, where relevant, set out how and why the information will be shared within the Council.

Data collected for a specific purpose e.g. council tax, cannot be used or disclosed for any other purpose without the permission of the data subject.

A privacy notice should state the following:

1. the name of the service e.g. Commercial Services
2. The purpose(s) for which the data is to be processed
3. Point to where more detailed information can be found e.g. weblink

12. SUBJECT ACCESS REQUESTS (SARS)

Individuals have a right to access information about themselves. Thanet District Council will disclose any information it holds (applying any appropriate exemptions) within 40 calender days of receiving a request and acceptable identification.

The Council will charge the current maximum £10 fee allowed for processing data access requests.

Every request for access, whether from the Council's own employees or the public, should be directed to the Data Protection Officer who will respond to all requests.

The SAR request form (with notes on completion) is attached at Annex 1

13. PERSONAL DATA HELD BY THANET DISTRICT COUNCIL

The Council's notification is available for inspection on the Information Commissioner's website: www.dpr.gov.uk/search.html.

The Council's number for accessing its entry is Z5398859.

Please note that for the purposes of this policy, 'data' includes all information including that held on physical files.

Personal data will be kept in an appropriately controlled and secure environment both within Council premises and if any such data is removed from Council premises.

14. TRAINING

Tier 2 Managers are responsible for ensuring that Thanet District Council's Data Protection Policy is communicated and implemented within their area of responsibility with appropriate levels of supervision.

All new and existing staff will undertake the "Ivysoft" training module on data protection and familiarise themselves with the DPA pages on TOM which will include guidance in the form of flowcharts, FAQs, and links to the relevant forms including our DPA Policy and Procedures. More in depth training will be provided to Tier 1 & 2 Managers and for other staff working in specialist roles.

A Managers Toolkit will be provided online as part of the 'Officers Handbook' due for publication in July 2011 which will also form part of the induction of new members of staff.

Each employee has an individual responsibility to be aware of their statutory responsibility for following good data protection practice.

15. BREACHES OF THE ACT

A breach of the Act may arise from a theft, accidental loss by an employee, a deliberate attack on the Council's systems, unauthorised use of personal data by an employee or equipment failure.

In the event of a breach staff should follow the Data Security Breach Policy (attached at Annex 2).

16. INFORMATION SHARING

Data sharing and/or processing with external agencies (including shared services arrangements and ALMO's) will be the subject of a written data protection agreement setting out the powers that permit the sharing/processing, its scope and controls and will be subject to approval by the Data Protection Officer prior to sign-off. If you are sharing data and the sharing is not clearly part of your routine statutory function, you must ensure that an appropriate agreement is in place. Contact the Data Protection Officer for further details and advice.

17. PRACTICAL GUIDANCE FOR MEMBERS AND OFFICERS FAQs

What does the Act mean for employees?

The Council is committed to compliance with the Act. Managers should ensure that their area of operation complies with the Act, that their use of personal data is registered (via the Data Protection Officer) and that staff are aware of the policy and procedures to be followed. This includes ensuring that all new and existing staff undertake the "Ivysoft" training module on data protection, have read and understood this policy document and are familiar with the Data Protection Act page on TOM. Each employee has an individual responsibility to be aware of what the Act involves and how to comply with it.

What does the Act mean for Members?
Elected Members should make themselves aware of and comply with this policy when engaged on Council work. Members must ensure that their use of personal data in their constituency work is registered with the Information Commissioner. There should be a clear separation between the data held for Council work and that held for constituency work.

How do I know if I can disclose personal data for a particular purpose?
Generally, data held by the Council is not to be disclosed outside the Council unless required by law. Disclosures within the Council are permitted if they are necessary for an officer to carry out their normal duty but the purpose must be compatible with the purpose for which it was originally gathered. There will be occasions when confidentiality will not allow even internal disclosure. Contact the Data Protection Officer for further information if you are at all uncertain about any specific situation.

How do I deal with requests from external organisations to share data?
All requests, whether from individuals or external agencies including for example the police, DWP or a Health Authority, should be passed immediately to the Data Protection Officer who will advise whether or not the request may be complied with. If any agency proposes a long-term partnership in data sharing, a written agreement must be prepared, stating what powers it has to enter into such an agreement, who will manage the exercise and what controls will be in place to protect the information. All such agreements must be approved and signed-off by the Data Protection Officer, who shall retain the original versions of such agreements on behalf of the Council. For detailed advice contact the Data Protection Officer. It should be noted that, if a request is made regarding an individual, the agency making the request should specify, in writing, why it requires the information, and the legal authority for requesting such information.

What about publicly available information?
When you receive a request, first check the Council's publication scheme to see if the information is already in the public domain. If you think this is the case, please advise the Data Protection Officer when sending the request to him.

What personal data does the Council hold?
The Council's notification is available for inspection on the Information Commissioner's website: www.dpr.gov.uk/search.html. The Council's number for accessing its entry is Z5398859.

What about manual/physical files?
Manual files are covered by the Act. Subject access to manual files is permitted and any processing that involves manual files must be notified to the Information Commissioner.

Can we carry out 'Data Matching'?
Data matching is the act of examining data held in two or more systems in order to check whether there is any recorded information common to both or all of those systems that indicates that the information relates to one and the same person. The Council may carry out data matching if there is a clear justification for it, such as the detection of fraud.

Does the Council disclose to the Police/DWP/Other Agencies?
Local Councils may disclose to other agencies for the purposes of the "prevention of crime or apprehension of offenders", anti-social behaviour and community safety as

permitted under Section 115 of the Crime and Disorder Act 1998. There is no general disclosure to external agencies. Again, all requests must be sent to the Data Protection Officer for processing/formal response.

Where may I obtain further information and advice?

1. See TOM – "The Data Protection Act"
2. Visit: www.ico.gov.uk/for_organisations/sector_guides/local_authority.aspx
3. If you require further assistance, please contact the Data Protection Officer, Harvey Patterson or his delegate, Gary Cordes in Legal Services.

Appendices

Appendix 1 Sars Form **+ notes**

Appendix 2 Breach Policy **+ Form**

Appendix 3 TOM Page

Appendix 4 Flowchart**: Managers Guide to Sharing Information**

Appendix 5 Checklist

Appendix 6 TDC Internet Page

Appendix 7 **Information Booklet for Customers**

Appendix 8 Privacy Statement