Corporate Services

Legal, Democratic and Regulatory Services

Data Protection Procedure

WDC Registration Number – Z6969445

Last Updated - November 2011

1 - Data Protection Procedure

2 - Compliance Advice

1 - Data Protection Procedure

1.1 Introduction

West Dunbartonshire Council is fully committed to compliance with the requirements of the **Data Protection Act 1998** ("the Act"). The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

1.2 Statement of Policy

In order to operate efficiently, West Dunbartonshire Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients, customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

West Dunbartonshire Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

1.3 The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;

6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between 'personal' data and 'sensitive' personal data.

Personal data is defined as, data relating to a living individual and which an individual can be identified from:

- The data held
- That the data which is held and with other information which is in the possession of, or is likely to come into the possession of the data controller and 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.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

1.4 Handling of Personal / Sensitive Information

West Dunbartonshire Council will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and 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 checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;

- Ensure that the rights of people about whom the information is held can 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 personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, West Dunbartonshire Council will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, 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;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All Elected Members are to be made fully aware of this policy and of their duties and responsibilities under the Act and to ensure that they are registered on the data protection register held by the Information Commissioner.

All managers and staff within the council's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and 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 the council and that individual, company, partner or firm;
- Allow data protection audits by the council of data held on its behalf (if requested);
- Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors 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 with regard to information supplied by the council.

1.5 Implementation

The Council has appointed a **Data Protection / Information Protection Officer**. Designated officers have also been identified in all directorates. These officers will be responsible for ensuring that the Policy is implemented.

Implementation will be led and monitored by the Data Protection / Information Protection Officer. This officer will also have overall responsibility for:

- The provision of cascade data protection training, for staff within the council.
- The development of best practice guidelines.
- Carrying out compliance checks to ensure adherence, throughout the authority, with the Data Protection Act.

1.6 Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. West Dunbartonshire Council is registered as such. The Council's registration number is **Z6969445**.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end the designated officers will be responsible for notifying and updating the Data Protection / Information Protection Officer of the processing of personal data, within their directorate.

Data Protection / Information Protection Officer will review the Data Protection Register with designated officers periodically, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Data Protection / Information Protection Officer immediately.

1.7 Subject Access Requests

A data subject is entitled at reasonable intervals and without undue delay or expense:

- to be informed by any data user whether he holds personal data of which that individual is the subject; and
- to have access to any such data held by a data user; and
- Where appropriate, to have such data corrected or erased

Data Users Responsibility

(a) Data Users must be able to satisfy the law that allows for Subject Access. Subject Access procedures must be established, and will be additional to those procedures that currently allow Data Subjects routine access to some of their own personal data. Data Users must, therefore, consider how Subject Access to personal data could affect their operations.

(b) Procedures to identify a Data Subject should be thorough, and appropriate to the sensitivity of the data. Details can be sought from the Data Subject to help locate the data in question. However, neither the verification nor the time taken must be excessive, and, once satisfied, procedures must allow for a copy of the Data Subject's data to be provided to them within 40 days.

(c) Procedures must provide for an explanation to be given of any codes, or other data not likely to be intelligible to the Data Subject. Following Subject Access, Data Users may have to allow rectification or erasure of personal data, in compliance with requests from Data Subjects (see the Fifth Data Protection Principle). This may involve some kind of appeals procedure.

(d) Advice, assistance and help with the interpretation of a Data Subject's personal data may be necessary in special circumstances, e.g. where a Data Subjects has English as a second language or has a disability which impairs reading.

(e) A fee may be charged by the Council for Subject Access; if so, a procedure must be established for handling such fees.

(f) N.B. It is essential that any Data User or Department that receives a Subject Access Request recognises it as such and notifies the Data Protection / Information Protection Officer immediately. The 40 days allowed for provision of data to the Data Subject is a legally binding timeframe. Subject Access is a legal right. Data Users must always seek the assistance of the Data Protection / Information Protection Officer when responding to Subject Access Requests.

Questions to Consider

- Are there any existing procedures whereby Data Subject can have access to their data?
- What are the procedures for verifying the identity of a Data Subject?
- How easy is it to locate personal data to which Subject Access is required?
- Is there any personal data contained therein that identify another individual? If yes, would these need to be deleted; or can you obtain consent from the other individual, before meeting the Subject Access request?
- Is there any personal data that contain other data which might be exempt from Subject Access? How do Data Users ensure that this information is not disclosed?
- Are all possible locations of data identified by the Subject Access procedures? (E.g. Structured Filing Systems and Personal Computers as well as Corporate Processors).
- Are there any codes or inferences in the personal data that require explanation? (bear in mind that data held in paper files is now subject to the Data Protection Act).
- Do procedures ensure that the Data Protection Officer is notified, and that the data will be able to be released with the prescribed 40 days?
- Are opportunities taken to make effective use of the Public Relations potential of Subject Access procedures?

2 - Compliance Advice

2.1 Introduction

This section sets out advice to assist Data Users comply with the provisions of the Data Protection Act. In particular, it is intended to:

- Assist management and other Data Users or Data Controllers, including Elected Members and agents of the Council to understand their obligations under this Act;
- Indicate the practical steps to be taken by Data Users to comply with the Act;
- Assist Data Users to understand how Data Subjects may exercise their rights under the Act, and what steps should be taken to reassure Data Subjects that their own personal data is always personally handled;
- Help to promote common standards within the Council with respect to all aspects of the use of personal data.

Each section of this document explains a Data Protection principle and what the principle means in practice, and ends with a series of questions for Data Users to check against their understanding and departmental procedures.

If Data Users are unsure on any aspect of any section, then they should discuss the matter with West Dunbartonshire Council's Data Protection / Information Protection Officer.

The Council's Data Users, through management and the Director or Head of Service must meet the obligations described below, and demonstrate compliance with the Data Protection principles. To ensure that working practices comply with the Act, a Procedural Review should be carried out where necessary. Departments must ensure that any procedure adopted to comply with any principle, includes a means of assessing that procedural effectiveness.

2.2 Specific Obligations to the Eight Data Protection Principles

2.2.1 The First Principle

"Personal data shall be processed fairly and lawfully"

Data Users Responsibility

(a) Data Users should ensure that any person from whom personal data are obtained is not misled as to the purposes for which such data are held, used or disclosed. An indication of the purpose(s) should appear on any form used to collect

data, and Data Users should be trained to explain, where necessary, why personal data is being collected and to whom data may be disclosed.

(b) Data Users should ensure that no unfair pressure is used in order to obtain the information, e.g. the implication that a service may be withheld unless a form is completed.

Procedural Review Questions to Consider

- From whom are the personal data obtained?
- How are they obtained? In confidence?
- Are people advised at the time of the information is obtained of the various purposes, uses or disclosures involved?
- Is your Department registered for the purposes intended for use?
- Do you need to redesign forms, or train Data Users in the proper techniques of obtaining personal data?

2.2.2 The Second Principle

"Personal data shall be held only for one or more specified and lawful purpose"

Data Users Responsibility

(a) Data Users must play their part in ensuring that the information which the Council has registered with the Information Commissioner, via Notification, is properly audited and kept up to date. This means that Departments must review, as necessary, the personal data used by the Council, to ensure that Departmental Register Entries contain:

- Particulars that adequately describe all processing of personal data;
- A sufficient explanation of the reason(s) for which the personal data is held;
- The sources, disclosures and types of personal data;

(b) Departments should be aware that the Council has designated a Data Protection / Information Protection Officer responsible for lodging notification with the Data Protection Registrar. However, the responsibility lies with Data Users to ensure that Council's Notification properly reflects the processing which is carried out within individual Departments. As it is the Notification that defines the legality of the use, collection or disclosure of personal data by each Department, any query or doubt should be discussed with the Data Protection / Information Protection Officer.

Procedural Review Questions to Consider

- Has a standard purpose been chosen?
- Does the standard purpose adequately explain the reason for which the data are held?
- How is a new purpose notified to the Data Protection Officer?
- How are the particulars in the Notification kept up to date?

2.2.3 The Third Principle

"Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes"

Data Users Responsibility

(a) Data Users must ensure that the terms 'adequate, relevant, not excessive' are properly considered with respect to data held. Departments should be prepared to justify why personal data is held, and undertake to ensure that any item of personal data is within the scope of the relevant registered purpose.

(b) Each Department should establish procedures which check the relevance of personal data, and be able to explain to Data Subjects why particular data is required.

Procedural Review Questions to Consider

- Can the reason for holding every item of data be justified?
- Is any item of data outside the scope of the registered purpose?
- Is any data held merely because 'they could be useful'?
- Is the data sampled, at regular intervals, to check its relevance?
- Is there a procedure to remove irrelevant personal data?

2.2.4 The Fourth Principle

"Personal data shall be accurate and where necessary, kept up to date"

Data Users Responsibility

(a) Data Users must ensure that adequate procedures exist to validate all personal data for accuracy, and to keep personal data up to date.

(b) Procedures must incorporate requirements for necessary corrections of personal data, to rectify or erase such data as may be necessary, and to advise disclosees of such changes whenever appropriate.
(c) Actions based on personal data later found to be inaccurate should be reviewed.

(d) Data Users must be aware that damages can be awarded against the Council as a result of its use of inaccurate personal data; therefore robust procedures for ensuring accuracy are extremely important.

Procedural Review Questions to Consider

- Are the personal data provided by the Data Subjects, by a third party or both?
- Is there a marker to indicate the source of the data?
- How are the data checked for accuracy?
- How often is such a check carried out?
- What procedures are used to rectify or erase personal data, in compliance with requests from Data Subjects and/or Court Orders?

- What procedures are used for verifying the accuracy of data input, or updating data where necessary?
- What degree of damage could be caused by inaccurate or out of date personal data?

2.2.5 The Fifth Principle

"Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"

Data Users Responsibility

(a) Data Users should establish procedures to review the length of time that personal data is kept, and to monitor whether personal data is still required. Bear in mind that certain data requires to be kept for a certain time to satisfy legislative requirements.

(b) Personal data that is no longer needed should be deleted. Where personal data is kept for historical or statistical purposes, a Data User should be prepared to justify the grounds for this decision.

Procedural Review Questions to Consider

- How often is personal data reviewed, to establish whether it is still required for its legal purpose?
- Are there legal or legislative requirements for keeping data for a certain length of time?
- Are there procedures to check when the data was obtained?
- In what circumstances would personal data be deleted?
- Can personal data, which is kept for historical or statistical purposes be 'de-personalised? (Please remember that the Act only covers personal data about living persons).
- How is data which is no longer needed deleted from systems?

2.2.6 The Sixth Principle

"Personal data shall be processed in accordance with the rights of data subjects"

Data Users Responsibility

(a) Data Users must ensure that;

- All disclosures are lawful and compatible with established procedures and Notifications;
- personal data are only disclosed after proper identification of the disclosee(s);
- All disclosures are regularly monitored and reviewed to see if they are appropriate;
- Data Users are at all times aware of the particular responsibilities pertaining to the disclosure of personal data, are properly trained, and will not disclose personal data without following established procedures.

(b) Each Department should establish procedures to record disclosures where appropriate.

Procedural Review Questions to Consider

- Are all disclosures compatible with established procedures, Notification Entries and Codes of Practice?
- How are these disclosures monitored and recorded?
- Are Data Users trained to cope with difficult enquiries?
- Do Data Users know how the Register Entries affect their day-to-day work?

2.2.7 The Seventh Principle

"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"

Data Users Responsibility

(a) Data Users must evaluate the security of personal data held by the organisation, taking account of the potential harm to a Data Subject that would result from a security breach, and implement appropriate security measures. Departments must ensure that security of personal data has a high priority and profile, as part of the Council's Security Policy. Staff training and the suitability of staff for particular posts must be considered as an integral requirement for ensuring personal data security.

(b) It follows that Data Users must ensure that equipment, data and documentation are secure, and that access to data and equipment is at all times restricted to appropriate staff. Departmental procedures should be monitored and reviewed and should include provisions for preventing accidental disclosures.

Procedural Review Questions to Consider

Physical Security

- Are the locations of all equipment on which personal data is held known to management?
- How is access to building and equipment safeguarded?

Software Security

- How is access to equipment, programs and personal data restricted to appropriate staff?
- How are magnetic media (e.g. floppy disks) used, stored and disposed of?
- How sensitive is the data?
- How is password security maintained?
- How regularly are access and usage monitored?
- Are security copies of programs and data taken and stored safely?

Printed Matter

- Where are documents (e.g. computer printouts) stored?
- How is computer output distributed?

- How is computer output disposed of?
- How is access to documentation controlled?

Contingency Planning

- Is personal data adequately backed-up in a secure location?
- What procedures, (including manual office procedures) are there to ensure recovery from fire, flood and other disasters?
- What procedures, (including manual office procedures) are there to cover lesser accidents, such as loss of personal data, unavailability of equipment or network, corruption of personal data etc.?

Staff Awareness

- What precautions are taken to prevent accidental disclosures?
- Are staff aware of security issues, the Council's Security Policy, and what training have they received?
- Who is responsible for the security of personal data?
- Do all staff know who is responsible for security within your department?
- How and when is security reviewed with your department?

Staff Reliability

- How is staff integrity evaluated prior to any activity that involves access to personal data?
- Are staff properly trained to process personal data?

Contracts

- Do the Conditions of Service embody a statement that informs staff of their responsibilities towards personal data held by the Council?
- Do contractors, external agents or consultants have in their contract with the Council a written obligation towards the requirements of the Data Protection Act?

2.2.8 The Eighth Principle

"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"

Data Users Responsibility

(a) Data Users must be able to satisfy the requirement that consent has been obtained from data subjects before publishing personal information on websites

(b) Users must not email personal information to destinations outwith the European Community unless they are satisfied that the recipient country has adequate Data Protection legislation.

Procedural Review Questions To Consider

- Are there any requirements to publish personal data on the Internet?
- Can you anonymise the information (e.g. using a title such as “the Secretary” of a group, instead of naming the individual)?
- Do you have written informed consent from each of your data subjects before publishing persona data on the Web?
- Does your Department or Section have a written, agreed procedure for the handling of and response to emails?

3 - Advice to Data Users on the Disclosure of Personal Data

3.1 Establishing Procedures

The following advice is intended to help Data Users establish procedures within Departments that will enable relevant staff to deal more easily and consistently with requests for a disclosure of personal data. These requests for information will come from Data Subjects; from with the Council (e.g. Members); or from Third Parties who can be any other body.

In the first and last cases, the procedures outlined below must be adhered to before personal data can be disclosed. However, internal disclosures of personal data can take place for bona fide purposes connected with the Data User’s functions within each Department.

In general, a disclosure must only take place if one of the following conditions applies:

- When the permission of the Data Subject has been given;
- Within the Council, for the authorised functions or Registered Purposes of the Council;
- to persons registered under the Data Protection Act as recipients (disclosees) of the Data User’s personal data (as specified in Registrations);
- Where the disclosure is by order of a Court, or a statutory duty.

3.2 Disclosing Personal Data over the Telephone

Staff should check the caller or the caller’s organisation against a list of authorised disclosees. If the person is described on the list, only information of direct relevance to their legitimate enquiry should be released. If the caller is not on an approved list, staff should not disclose any personal data, but discuss the matter with their line manager.

Staff should not disclose information over the telephone before the caller’s identity has been verified (e.g. by phoning them back on a known number, or by confirming a known reference number, or by discussing some reference details known only to

the Data User and the caller). This may be difficult if the caller is agitated or angry, but usually callers will divulge information that will help to assess their true identity.

If the caller is insistent or 'difficult', staff should ask whether it is possible for the caller to phone again, or to be phoned back at a later stage, or whether the caller can wait until staff can consult their line manager. Staff should try to be patient and calm.

3.3 Records

All disclosures of sensitive information may have to be recorded on the appropriate files or case papers.

Staff should be trained to ensure that all requests for personal data outwith their normal duties are approved by their line manager before the request is satisfied.

Staff must note that the confidential nature of any personal information supplied must be stressed at all times. They should not take short cuts and should always follow the correct procedure. If in doubt, do not disclose.

4 - Refusing to Disclose Personal Data

Staff should be polite and explain that they are not allowed to disclose personal data unless the caller's credentials to receive the data have first been verified. Staff should always explain that the reason why they are refusing to give information is one of confidentiality, and because the caller has not provided adequate identification. The following is suggested as the basis for a standard explanation:

'The Data Protection Act regulates the use of personal data. It is the Council's policy to respect the confidentiality of the personal data in our possession, and because you have not been able to identify yourself adequately, I cannot help you on this occasion. However, if you call again, or write to the Council and provide satisfactory identification, I should be able to comply with your request'.

5 - Disclosures of Personal Data to Prosecuting Agencies

If staff receive a request for personal data from a police officer, customs official, sheriff officer etc., they should refer the request to their line manager who will refer to the established procedure of that Department. Note that if the Data User has a statutory duty to provide personal data to these agencies, or if the data requested is not personal data subject to the Data Protection Act, then the following procedures need not be followed.

Section 28 of the Data Protection Act allows for personal data to be disclosed to certain agencies (e.g. Police, Inland Revenue, Customs & Excise, Public Health Authority, etc.) for the purposes of:

- ‘The prevention or detection of crime;
- The apprehension or prosecution of offenders; or
- The assessment or collection of any tax or duty’

Without fear of making an unauthorised disclosure so long as Data Users can prove that they ‘had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those purposes immediately above.

It is for senior management, usually at Director or Senior Manager level to decide whether to disclose personal data to these agencies. Note that there is no compulsion to comply with a request for personal data under this Section, and a request can be refused. In order to be consistent, all agencies who may want Data Users to disclose personal data under Section 28 of the Data Protection Act should be required to present a request in writing. Disclosures of personal data to such agencies should never be made orally.

If the disclosure is approved by senior management, a formal record should be made of the decision and file this with the written request. The record should include the time and date of the approval, who made the decision, who was involved about the disclosure discussions, and a copy of the personal data disclosed.
If the disclosure is denied, a formal note explaining why the personal data was not released should be sent to the agency, with a copy to the Chief Executive, in the event of any subsequent legal proceedings.

If a senior manager is unsure what to do, he or she should:

- Discuss the matter with their Director or the Chief Executive ;
  And
- Attempt to find out further information from the agency as to why the personal data is required.

6 - Emergencies

There may be circumstances where staff have to disclose personal data in emergencies. If an emergency involves a threat to a Data Subject’s health or to prevent injury to a Data Subject, then the disclosure can take place (by virtue of Section 34(8) of the Act).
A proper record of the disclosure must be made, either at the time, or a soon as possible after the disclosure has occurred. In other urgent situations, staff will have to use their judgement; but in all cases they should keep a formal record of their decision to disclose, and send a note of the disclose to their line manager.

Staff may be contacted by an individual who wishes to apply formally for Subject Access. In these cases, the Data Subject should be referred to the appropriate

person within each Department, and the Data Protection / Information Protection Officer should be notified as soon as possible.

All staff should be aware that Subject Access is a separate and formal procedure by which personal data is disclosed to the Data Subject.

7 - Responsibilities of Directors / Heads of Service

Directors / Heads of Service should supervise their staff in relation to disclosures of personal data, and ensure that staff are trained in the correct Departmental procedures. Line managers should liaise with the Data Protection Officer to ensure that staff have available to them a list of:

- Disclosures that are registered under the Data Protection Act;
- Disclosures that can be made but need not be registered under the terms of the Data Protection Act.

All other disclosures of personal data may be illegal. Consequently, should a line manager conclude that a disclosure, not covered by the points above, is required, reference should always be made to the Data Protection / Information Protection Officer before the disclosure proceeds.

8 - Access to Personal Data by Councillors or Elected Members

Staff should refer any request for personal data, from Councillors or Members, to their Line manager.
The common law principles concerning elected Members can be summarised as follows:
An Elected Member, by virtue of his/her office, is entitled to have access to all documents in possession of the Council as far as such access is reasonably necessary to enable him/her properly to perform his/her duties.

- A Councillor has no 'roving commission' in respect of Council documents and mere curiosity is not a sufficient basis for access to information.
- In the case of a Committee of which the Councillor is a Member, there is a presumption that the Councillor has good reason for access to all the information and documents which pertain to the functions of that particular Committee.
- In the case of a Committee of which the Councillor is not a Member, he/she has no automatic right of access to material and has to demonstrate a 'need to know'.
- The decision about whether a Councillor has good reason for access to the material of a Committee of which he/she is not a member is ultimately one to be taken by the elected Members themselves. Initially such a decision is likely to be made by an Officer, but in practice should be made by the Director concerned.

Where the Director is of the opinion that the 'need to know' obligation has not been demonstrated, a preliminary discussion with the Chief Executive should take place prior to the Member concerned being advised.

9 - General Advice to Elected Members

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the holding and processing of personal data, that is information relating to living individuals, which is held either on computer or in some cases in manual form.

The Act gives enforceable rights to individuals (data subjects) and places obligations on those legal persons who control the manner and the purpose of the processing of personal data (data controllers). Data controllers must notify the Data Protection Commissioner of the details of their processing. These details are published by the Commissioner in the register of notifications.

Data controllers must also comply with eight data protection principles, which together form an enforceable framework for the proper handling of personal data.

9.1 - Notification

In considering whether they need to notify, Elected Members must decide in which capacity they process personal data.

• As members of the Council they may have access to and process personal data in the same way as employees. The data controller is the Council rather than the elected member. An example is of a member of a housing committee who has access to tenancy files for the purpose of considering whether or not the Council should proceed with an eviction. In this case the elected member is not required to notify.
• When Elected Members act on their own behalf, they are likely to have to notify in their own right. Examples include the processing of personal data in order to timetable surgery appointments or progress complaints made by local residents. When campaigning within their own political parties for adoption as a prospective candidate for a particular ward they also act as individuals and can only rely upon the notification of their parties if as a matter of fact the parties control the manner and the purpose of the processing of personal data for the purpose of their individual campaigns.
• When acting on behalf of a political party, however, for instance as an office holder or as an official candidate, members are entitled to rely upon the data protection notification made by the party.

There is an important exemption from notification where the only personal data, which are processed, take the form of non-automated or manual records. However, even if this is the case and there is no notification requirement, elected members must comply with the other requirements of the Data Protection Act, in particular meeting the standard set out in the 8 data protection principles.

9.2 - Use of Personal Data

When considering whether it is permissible to make use of personal data for any particular purpose, elected members must first consider the context in which that information was collected, and in particular, who is the data controller for the data.

• Information, which is held by the local authority, may not be used for political or representational purposes unless the individuals to whom the data relate (the "data subjects") have agreed. Thus it would not be permissible to use a list of the users of a particular Council service (e.g. members of libraries) for electioneering purposes (e.g. a campaign against the closure of public libraries) without the consent of those individuals. Similarly it would not be permissible to use personal data to which the elected member had access in an official capacity, say as a member of the Housing Committee, in order to progress complaint on behalf of a local resident unless all the individuals concerned had consented.
• When campaigning for election as the representative of a political party, candidates may make use of personal data held by their parties such as mailing lists and of personal data, which they hold as elected members. For instance, it would be permissible to seek support from local residents whom the candidate has assisted in the past as a councillor. It would not, however, be permissible to disclose the details of those local residents to the party without consent.
• When campaigning for election to an office within a party, it is only permissible to make use of data controlled by the party if authorised to do so by the party and its rules. It would be wrong, for instance, to make use of information, which the candidate might have, in his or her capacity, say as the local membership secretary unless the party itself had sanctioned this.

9.3 - Offences

The Data Protection Act contains a number of criminal offences. In particular:

• Processing personal data unless a notification has been made to the Commissioner - An Elected Member who made use of a computerised list of library members or tenants for electioneering purposes would commit an offence if her or she had not notified.
• Making disclosures of personal data, which have not been authorised by the data controller - An Elected Member who disclosed personal data to his or her party for electioneering purposes would potentially commit this offence.
• Procuring unauthorised disclosures of personal data - An Elected Member who obtained a copy of personal data ostensibly for council purposes but in reality for his or her personal use or the use of his or her party would commit an offence.

9.4 - Further Advice

Further general advice on the data protection Act is available from the Commissioner's office and from the website (http://www.ico.gov.uk/) or via the Information Line (01625 545745).

More comprehensive advice for elected members is available from the Improvement and Development Agency (IDeA) http://www.idea.gov.uk).