DATA PROTECTION: A COUNCILLOR’ S GUIDE

CONTENTS

PREFACE ............................................................................................................... 4
INTRODUCTION .................................................................................................. 5
SUMMARY ......................................................................................................... 6
DATA PROTECTION AND THE COUNCILLOR - CHECKLIST........................... 7
Councillor as Processor of personal Data as part of their Council functions ... 7
DATA PROTECTION AND THE COUNCILLOR - PART 1 .................................... 9
INTRODUCTION ................................................................................................ 9
ROLES, RESPONSIBILITY AND DUTIES OF A COUNCILLOR......................... 9
PART II ................................................................................................................ 11
THE DATA PROTECTION ACT 1998 – Questions and Answers........................ 11
What is it? ........................................................................................................ 11
What does it do? ............................................................................................. 11
What manual data are covered by the Act? .................................................. 11
What is a relevant filing system? ................................................................. 11
Can a Councillor be a data controller? ......................................................... 12
Are there any examples of purposes that entitle the Councillor

to be regarded as the data controller? ......................................................... 12
What are the implications for a Councillor who is also a data controller? .... 12
What does Notification require? ............................................................... 13
What is the position of the Councillor who receives information from

his authority as part of his/her function as a local Councillor? .................... 13
THE DATA PROTECTION PRINCIPLES ............................................................ 14
Controllers are required to comply with the Data Protection Principles. What are the

principles? ....................................................................................................... 14
How do I ensure that I comply with the principles? .................................. 14
The First Principle ........................................................................................ 14
Do we always have to obtain the subject’s consent? ................................ 14
What does consent require? ................................................................. 14
Does consent need to be in writing? ........................................................ 14
Do we need to have consent for every purpose for which

we require personal data? ........................................................................ 15
What is explicit consent? ............................................................................... 15
The Second Principle .................................................................................... 15
The Third Principle ...................................................................................... 15
The Fourth Principle .................................................................................... 15
The Fifth Principle ...................................................................................... 16
The Sixth Principle ...................................................................................... 16
The Seventh Principle .................................................................................. 16
Eighth principle ........................................................................................... 17
PART IV ............................................................................................................... 18
DISCLOSURE OF DATA BY AUTHORITY TO COUNCILLORS........................ 18
PART V – RIGHTS OF THE DATA SUBJECT .................................................. 21
APPENDIX A ..................................................................................................... 23
THE DATA PROTECTION PRINCIPLES ............................................................ 23
APPENDIX B ..................................................................................................... 24
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF ANY PERSONAL DATA .................................................. 24
CONDITIONS RELEVANT FOR THE PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE
PERSONAL DATA ........................................................................................... 25
APPENDIX C ..................................................................................................... 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAWFUL PROCESSING</td>
<td>27</td>
</tr>
<tr>
<td>APPENDIX D</td>
<td>29</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>29</td>
</tr>
<tr>
<td>Accessible record</td>
<td>29</td>
</tr>
<tr>
<td>Data</td>
<td>29</td>
</tr>
<tr>
<td>Data Controller</td>
<td>29</td>
</tr>
<tr>
<td>Data Subject</td>
<td>29</td>
</tr>
<tr>
<td>Subject Access</td>
<td>29</td>
</tr>
<tr>
<td>Personal Data</td>
<td>29</td>
</tr>
<tr>
<td>Processing</td>
<td>29</td>
</tr>
<tr>
<td>Recipient</td>
<td>30</td>
</tr>
<tr>
<td>Relevant Filing System</td>
<td>30</td>
</tr>
<tr>
<td>Unstructured personal data</td>
<td>30</td>
</tr>
</tbody>
</table>
The guide and the briefing note have been written by the IDeA’s Rights in Data working group. The group comprises:

<table>
<thead>
<tr>
<th>John Hanafin, (Chair), Elmbridge Borough Council</th>
<th>Edwina Withe, Bracknell Forest Borough Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Taylor, Bristol City Council</td>
<td>Margaret Ingram, Congleton Borough Council</td>
</tr>
<tr>
<td>Stuart Lynch, Metropolitan Borough of Wirral</td>
<td>Alison Sutherland, Local Government Association</td>
</tr>
<tr>
<td>Barry Adams, East Riding Council</td>
<td>Dougie Youngson, Edinburgh City Council</td>
</tr>
<tr>
<td>Nicola Wood, Improvement &amp; Development Agency</td>
<td>Ian Lebbon, Flintshire County Borough Council</td>
</tr>
<tr>
<td>Alan Graham, Stirling Council</td>
<td>Ray Brown, London Borough of Waltham Forest</td>
</tr>
</tbody>
</table>

The group would particularly like to thank Ian Robertson for his contribution to this document.
INTRODUCTION

All Councillors will have been affected by the growth in the number and power of information systems and the use of the internet. They will also have been involved in developments such as the extensive use of CCTV. The Data Protection Act 1998 has introduced important changes to data protection law. It is a good time then to update advice to Councillors on the requirements of the Data Protection legislation. This guidance also takes account of the changes brought about by the Government’s modernising agenda, such as the issues of joined up government, partnerships, public consultation and changes in the political management structures.

The 1998 Act extends the scope of data protection to manually processed personal information as well as that processed by automated means. It gives people improved rights, and it imposes greater controls on individuals and organisations who hold personal data about individuals, and brings CCTV within the scope of the legislation. Councillors are therefore affected by the changes introduced.

Councillors are likely to hold personal data for a variety of purposes: as ward Councillors, in decision making, in deciding appeals, as members of bodies external to the council. Whether exercising an Executive role, or as a member of Scrutiny committee, Councillors need to ensure that procedures are in place for data protection security measures and that they are adequately resourced.
SUMMARY

This guidance is in five parts.

1. Part one is a general section consisting of an introduction, a brief note covering the scope of the guidance and a discussion of the various roles, responsibilities and duties of a Councillor and how these affect his/her status in data protection terms. In discussing the Councillor’s role, account is taken of the fact that he/she may be involved with other organisations or activities by virtue of being a Councillor.

2. Part Two deals with a few general questions raised by the Act and provides definitions of the main terms which appear in it.

3. Part Three examines more closely the implications of the new Act for Councillors, concentrating in particular on the need to notify and compliance with the principles. As the principles underpin the whole Act these are dealt with in some detail.

4. Part Four discusses disclosure to Councillors

5. Part Five deals with the Councillor and the Data Subject.

This Guidance also contains three appendices:

Appendix A is a list of the of the Data Protection Principles.

Appendix B is about the Conditions relevant for the purposes of the first principles to the processing of personal data, including sensitive personal data.

Appendix C relates to Lawful Processing.
DATA PROTECTION AND THE COUNCILLOR - CHECKLIST

Councillors are likely to hold and ‘process’ personal information on individuals in different capacities – for their own purposes and for the purposes of council business.

Councillor as Data Controller

1. The Councillor will be regarded as the “data controller” for the purposes of the Data Protection Act when he/she:

   processes personal data on his/her own computer for his/own purposes.

   is processing data for his/her own purposes on equipment supplied by the authority. Examples of uses which may qualify the Councillor as data controller include:

   a) Details of complaints
   b) Details of cases where the Councillor is acting on behalf of a constituent
   c) Personal data held for constituency purposes
   d) Lists of contacts
   e) Data held as part of the Councillor’s duties as a representative of a national body
   f) Data used for political canvassing

2. Councillors regarded as the data controller must notify the Information Commissioner of all of the purposes for which they hold and process personal data on computer. Notification is for one year, requires a fee of £35.00, and is renewable annually

3. The Councillor must also notify the Commissioner of any changes in his/her notified particulars.

4. As a Data Controller, the Councillor must comply with the data protection principles. These are set out in Appendix A.

5. It is an offence for a data controller to process personal data on a computer without having notified the Commissioner. Prosecution could result in an unlimited fine if tried in the Crown Court.

6. Complying with the data protection principles requires the Councillor to provide an individual with details of the personal data required, the purposes for which it is processed, a note of the recipients to whom the data may be disclosed, and details of any statutory purpose governing his/her processing of the data. In short, sufficient information to enable the individual to understand why the Councillor is processing the data.

   The Councillor should take steps to ensure that the personal data he/she processes is accurate, up to date, sufficient for its purpose(s), is not kept for longer than is necessary and is held securely and cannot be accessed by others when it is not in use.

Councillor as Processor of personal Data as part of their Council functions

The Councillor is likely to receive personal data about individuals from the local authority in order to enable him/her to carry out the duties as a member of the council. Where this occurs, the
Councillor’s use of the data is subject to the conditions governing the authority’s use of the as though he/she were an employee.

A Councillor who processes data provided by the council on his/her own computer may be regarded as a "Data Processor" - that is a person who processes the data on behalf of the controller (the council). As a data processor the Councillor is not required to notify the commissioner but must comply with the principles of the Act.

The Councillor’s role may vary, depending on whether or not he/she is a member of the Executive or on a Scrutiny or Standards Committee. When exercising any role, Councillors must ensure that Data Protection legislation is complied with. Members of the Executive who propose the budget should ensure that adequate provision is made for relevant data protection and security measures.

A Councillor serving on an external body will be subject to any conditions and restrictions covering the external body’s processing of personal data including any policies and procedures.

Councillors who are data controllers are required to provide data subjects with a copy of the personal data they process about them on request. The data provided should not include information about or identify other individuals unless permission has been sought first.

The Councillor must also correct, erase, block or destroy data which the subject has shown to be incorrect or if ordered by the Court to do so. Where data has been disclosed to a third party, that person should be informed of the action taken.

The Councillor is responsible for ensuring the security of the personal data which he/she holds and processes. The level of security he/she provides should be adequate for its purpose. Advice on an appropriate level may be sought from the authority's Data Protection Officer.

A Councillor is entitled to have access to any information necessary to enable the conduct of his/her statutory duties as a Councillor. Councillors do not, however, have the automatic right to access any data and personal data will only be disclosed where there is a recognised need (e.g. as a member of a specific committee or when acting on behalf of a constituent).

Councillors should always treat personal information provided to them for council business, or collected by them when acting on behalf of a constituent, as having been provided in confidence. It should not be disclosed to third parties unless permission has been sought from the individual.
PART 1 - DATA PROTECTION AND THE COUNCILLOR

INTRODUCTION

The Data Protection Act 1998 has an impact on Councillors and the way that they perform the many functions that are part and parcel of their daily lives. This legislation, unlike its predecessor (the Data Protection Act 1984) - which applied only to personal data processed by automated means - regulates the processing of information relating to individuals, by both manual and automated means.

Although advances in the use of IT are making technology indispensable to Councillors in the performance of their duties, personal information may still be held and processed manually. As a result the Councillor needs to be aware of the changes brought about by the new Act and their effect on the way that he/she performs the function of local Councillor.

Because of the many different roles that Councillors are required to play their status, in data protection terms, will vary. This can and does lead to confusion and a misunderstanding of the Councillor’s rights and legal obligations; a situation not helped by the Councillor’s status in law. For this reason, therefore, this guidance is designed to assist Councillors and also those who advise them.

The purpose of this document is to provide guidance to Councillors and a general framework within which local authorities can operate when preparing local rules and codes of practice.

The Nolan Commission on Ethics in Government has stressed the need for such measures.

ROLES, RESPONSIBILITY AND DUTIES OF A COUNCILLOR

The following definition is used to describe the Councillor for the purpose of this Guidance:

“The Councillor is the elected representative of his/her constituency and as such is expected to act “according to the best of her/his judgement and ability” in the interests of constituents’.

Councillors, by virtue of their office are required to fulfill a number of different roles, each with its own duties and responsibilities. As the nature of these varies so too does the relationship between the Councillor and the Data Protection Act.

In Data Protection terms, the Councillor can find him/herself being treated as any of the following depending on the particular role and circumstances in which she/he is operating:

a) An employee of the authority and therefore subject to the conditions attached to the authority’s purposes and processing of personal data.

b) A Data Controller in his/her own right

c) a Data Subject

d) an agent/intermediary/advocate acting on behalf of another individual.
The various roles performed by the Councillor are described, briefly below.

**The primary role of the Councillor is that of Councillor.** As such she/he is elected to represent a particular group of citizens on the council and its several committees. The administration and decision making processes in local government are subject to a number of statutes which are binding on the Councillor who is also required to comply with the National Code of Local Government Conduct (which is soon to be replaced) and local Standing Orders (which will be replaced by Procedural Rules under the new constitutional arrangements) and in some cases local codes of conduct. In Data Protection terms a Councillor performing his/her statutory duties is regarded in the same way as any employee of the authority.

**The Councillor may also sit as the Council’s representative on a number of outside bodies**

He/she may sit on the Board of a Housing Company, or a Housing Association, as a trustee, of a charitable trust, as a school governor or on a village hall committee. The Councillor’s duties will vary depending on the role taken but in the case of a Trustee or Director they will owe a duty to the organisation on which they sit.

**Councillor may also be required to act as the authority's representative on other public sector bodies, joint boards, working parties etc.** He/she may also represent the authority on local government national bodies (the Local Government Association (LGA), the Convention of Scottish Local Authorities (COSLA), the Improvement and Development agency (IDEA), the Local Government International Bureau (LGIB) and Local Authority Committee on Trading Standards (LACOTS) are all examples. As long as the Councillor is representing the Council his/her status will be the same as any employee of the council serving in a similar capacity.

**Where Councillors, are required to act as the Authority's appointed representatives on local government national bodies,** the Councilor’s responsibility will be towards the body which made the appointment and not the home authority in the first instance.

The majority of Councillors are members of a specific political group/party and will be subject to any conditions established by the organisation concerned in respect of the processing of personal data for its purposes.

Councillors are also Data subjects and have the same entitlements as any other individual under the Data Protection Act, regarding personal information held about them.
PART II
THE DATA PROTECTION ACT 1998
QUESTIONS AND ANSWERS

What is it?

“An Act to make new provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information”.

This measure applies to both the manual and automated processing of such Information (i.e. personal information held on computer and in manual filing systems)

What does it do?

It replaces the 1984 Data Protection Act, and the Access to Personal Files Act 1989 which entitled individuals to access personal data held on manual files for housing and social services purposes – and access rights granted in other legislation such as those granted to pupils and parents under the Education Reform Act 1988.

• It requires all those who process personal data to comply with the eight data protection principles that provide the basis of the Act.

• It gives individuals (data subjects) enhanced rights.

• It establishes conditions applying to the fair and lawful processing of personal data including the need to seek the consent of the individual to the processing of personal data about him/her where none of the other conditions can be met.

• It prohibits the processing of sensitive data other than for certain specified purposes.

• It introduces the terms ”relevant filing system“ and ”accessible public record“

• It provides for exemptions in specified cases.

• It replaces the term ”Data User“ with that of ”Data Controller“

• It created the role of the Data Protection Commissioner, who is now known as the Information Commissioner.

What manual data are covered by the Act?

All personal information which is part of a filing system or which is intended to become part of a filing system.

What is a relevant filing system?

The Act describes this as any set of information structured by reference to individuals or that can be accessed by reference to criteria relating to individuals. The Information Commissioner has described a “set of information” as comprising a group of things under a common heading or identifier. Files headed: Constituents, Contacts, Complainants could meet the criteria.

The personal data must also be capable of being accessed by reference to the individual or criteria
relating to the individual. For example: the individual’s name, a correspondence ref. number. or a
file number, address, age, membership of an organisation, (e.g. trade union, political party).

Files concerned with matters of council policy are unlikely to fall within this definition.

Councillors are advised to examine their manual and computer files to determine if they meet the
above criteria. There may be examples where, although the files contain personal data, the
information contained in them cannot be accessed by reference to an individual or by criteria
identifying any individual.

In carrying out such an examination Councillors are advised to seek the advice of the
authority’s Data Protection Officer.

Can a Councillor be a data controller?

Councillors will be data controllers whenever they process personal data for their own
purposes. This will be the case whether or not the Councillors are processing the data on their own
computing equipment or for their own purposes on the authority’s equipment.

Are there any examples of purposes that entitle the Councillor to be regarded as the data
controller?

Purposes for which Councillors may require and process personal data and which qualify them as
data controllers include:

A. Constituency Case Work
   This can include: the maintenance of constituents’ complaints and enquiries including details of
   any follow up action and the outcome; details of particular cases where the Councillor is acting
   as agent/ intermediary on behalf of individual constituents; personal data held for constituency
   purposes not necessarily connected with those of the council or the political organisation of
   which the Councillor is a member.

B. Canvassing Political Support:
   Included under this heading are: lists of contacts; personal information held for party political
   purposes;

C. Processing of personal data held in connection with his duties as a representative of a national
   body

D. Processing of personal data held and processed as part of the Councillors own business or
   profession.

The above is not an exhaustive list and has been prepared as an indication of the various purposes
for which the Councillor may require to process personal data.

What are the implications for a Councillor who is also a data controller?

• The Councillor must ensure that his/her processing of personal data complies with all of the
  requirements of the Data Protection Act:  the eight principles; the conditions attached to
  processing; the restriction on the processing of sensitive data; the rights of data subjects; the
  requirement to notify; the Commissioner’s notices etc.

• Councillors processing  personal data for any of the above purposes, by automated means –
desk-top, lap-top or hand held computers – are required to notify the Commissioner and have
the details of their notification entered on the Register of Notifications. The register is a public document.

- Those who maintain only manual records are not required to notify the Commissioner of the processing. They are, however, required to comply with all of the other requirements of the Act mentioned above.

**What does Notification require?**

Those who had registered their purposes under the 1984 Data Protection Act will find the new notification procedure much simpler. Notification requires the data controller to provide the following **“registerable particulars”:**

- his/her name and address;
- a general description of the personal data being/or to be processed;
- the categories of data subject to which the data relate (e.g. constituents);
- a description of the purposes for which the data are processed;
- a description of any recipients to whom the data may be disclosed.
- In addition a general description or statement of the security measures taken to protect the personal data is required. This latter does not appear on the public register.

Any data controller will have only one entry, so it is important to ensure that all of the purposes for which he/she is processing the personal data as a data controller, are included.

A fee of £35 must accompany the notification. The period of notification is one year after which, unless the processing has ceased, a continuation fee of £35 per year is required.

Failure to notify your purposes or changes to your notified particulars is a criminal offence.

Such offences are triable either in the Magistrates’ Court or the Crown Court. Offenders are liable to fines of up to £5,000 in the former or an unlimited fine in the latter.

If you are unsure of whether or not you should notify the Commissioner, the advice of the authority’s Data Protection Officer should be sought, in the first instance. You may wish to seek the advice of the Commissioner. Advice on notification is available by telephoning the Notification Hotline on – 01625 545 740

**What is the position of the Councillor who receives information from his authority as part of his/her function as a local Councillor?**

In this instance the Councillor will be a recipient of the information. Councillors will be included in the authority’s notified particulars as recipients of council information. Councillors must only use the data provided by the authority for the purpose(s) for which it was provided. Councillors who retain the information on their own computers or in a manual filing system must comply with procedures established by the authority. The authority should advise Councillors on these matters, and if in doubt – ask your authority’s Data Protection Officer.

**Any purpose or disclosure outside those that have been notified by the authority will be a breach of the Act.** It is a criminal offence for Councillors to used data provided by the Council for Council work for quite a different purpose (i.e. a database containing the names and addresses of residents who use the public library for political canvassing).
THE DATA PROTECTION PRINCIPLES

Controllers are required to comply with the Data Protection Principles. What are the principles?

These are the rules and conditions governing the obtaining, processing and maintenance of personal data. There are eight principles and they apply to all personal data processed by data controllers. Compliance with the principles applies equally to automatically and manually processed data.

A list of the principles accompanies this guidance (Appendix A).

How do I ensure that I comply with the principles?

Many local authorities have produced guidelines on the importance of complying with the principles and setting out controls and procedures covering all aspects of processing, from obtaining personal information to disposal, including procedures for security and for dealing with access requests. Councillors should obtain a copy of these and seek the advice of their authority’s Data Protection Officer where clarification is required. Information is also available from the Information Commissioner’s web site, www.dataprotection.gov.uk.

The First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a. At least one of the conditions in Schedule 2 of the Data Protection Act is met, and
b. In the case of sensitive personal data at least one of the conditions in Schedule 3 of the Data Protection Act is met

The first principle establishes the conditions attached to the fair and lawful processing of all personal data. Additional conditions apply where sensitive data items are to be processed. These are described in detail in Appendix B to this guidance. One of these conditions is that the data subject has given consent to the processing. In the case of sensitive data such consent must be explicit.

Do we always have to obtain the subject’s consent?

No, the data subject’s consent is required only when none of the other conditions for processing can be satisfied (See Appendix C).

What does consent require?

The subject needs to be given enough information to enable him/her to understand why the personal data requested are necessary. Clearly people must not be deceived or misled as to any purpose.

Does consent need to be in writing?

No. Consent does however imply that some form of communication has taken place with the individual. This can be achieved by completion of a form, a written document, (a letter) a fax an e-mail or even verbally. Councillors are advised to obtain written consent wherever possible.
Do we need to have consent for every purpose for which we require personal data?

Yes. Just because consent has been obtained to hold the personal information for one purpose, it must not be assumed that the subject has no objection to you using the data for other purposes. The only exception will be where you are required by law to process the data.

Constituency case work and canvassing political support for personal data obtained from the individual may only be processed with the consent of the subject. This implies that the individual has been provided with sufficient information to enable him/her to understand why the data are required. The Councillor must therefore ensure that whenever personal data are being obtained from constituents that the individuals are provided with sufficient information about why it is being collected and have no objections to this use.

Councillors passing on complaints and enquiries to local authority departments/services must inform the individual that personal data about him/her will be processed and held on file by the authority for the purpose of dealing with the complaint/enquiry and that the individual has a right to ask to see the data held.

What is explicit consent?

Explicit consent is one of the conditions attached to the processing of the sensitive data items.

The Second Principle

*Personal data 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.*

This means that personal data obtained for one purpose must not be used or disclosed for any purpose which is not compatible with the original purpose for which it was obtained.

Much of the information received by members for the conduct of council business is governed by other statute. Many of these restrict the use and disclosure of personal data to the purpose(s) of the service covered by the statute. It is not primarily the Data Protection Act which prevents them from sharing data. It is the legal framework, in which they and their local authorities operate, which can act as a constraint on data sharing.

The Third Principle

*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*

The message behind this principle is simple: personal information held and used for any purpose must only be that which is absolutely necessary.

The Fourth Principle

*Personal data shall be accurate and where necessary kept up to date.*

**NOTE:** A data subject has the right to ask the Court to order the correction, erasure, blocking or destruction of inaccurate data held about him/her. Those who are data controllers should also note that the Court may also order data controllers to inform third parties to whom data have been disclosed that any or all of these actions have taken place.
The Fifth Principle

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

This is clearly a reminder that once the Councillor has no further reason to retain personal information he/she should dispose of it. Information required for constituency and canvassing purposes need not normally be held for longer than its purpose.

**Councillors are advised to consult the local authority’s retention policies before disposing of personal data held for any purpose.**

The Sixth Principle

*Personal data shall be processed in accordance with the rights of Data Subjects under this Act.*

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.*

This principle covers the security of personal data. The level of security required will depend on the sensitivity of the data and the purpose for which it is processed.

Data Controllers

Councillors who are data controllers in their own right are responsible for ensuring that personal information is held securely.

Listed below are some good practice points

**Manual Records**

Use lockable filing cabinets, especially for storage of confidential information.
Lock all papers away securely when not in use, to prevent other people, including family members from gaining access.
Dispose of council information, confidential information and information about individuals according to the authority’s guidance on disposal.

**Computerised Records**

Access should be controlled by a unique password known to and used only by him/herself;
Passwords and access controls should be kept secure when not in use;
Personal information should not be left displayed on screen when not in use;
Floppy discs/CD ROMS should be filed away securely and not left lying around.
Where the computer used is also used by other family members they cannot access information relating to the Councillor’s Council, constituency or political duties
If the personal information is held on a lap-top computer this should be locked away when not in use.
Hard copy(print-out) of information should be filed securely or shredded when no longer needed.
This advice also applies to Councillors who hold and process information provided by or on behalf of other external organisations on which they serve. The Councillor’s processing of the data provided will be subject to the security requirements of the particular organisation. In any event information provided by these other organisations should be kept separate from all other information held and processed by the Councillor.

Councillors who are not aware of the local authority’s security requirements should ask the Data Protection Officer for a copy and advice and guidance on implementing it for his/her own processing and purposes.

Eighth principle

*Personal data shall not be transferred to a territory or country 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.*
PART IV

DISCLOSURE OF DATA BY AUTHORITY TO COUNCILLORS

Disclosure of information to Councillors is essential if they are to carry out their (statutory) duties as a member of the council. Such data may include items of personal data. In the terms of the Data Protection Act, Councillors will be described as “recipients of the information”. Councillors will be included in the local authority’s notified particulars as recipients, to cover all cases where the data concerned are processed by automated means. Data subjects requesting access to personal data processed about them will be told.

Disclosures to Councillors for the purposes of determining policy and ensuring the smooth running of the authority or as a member of a particular committee will therefore be included in the authority’s notified particulars.

Personal data received by Councillors from the authority remains the property of the authority, as data controller, and cannot be used or disclosed by the Councillor for any other purpose other than that for which it was provided.

The Councillor’s use is subject to any controls/procedures established by the authority covering the use of personal data and must be kept secure in line with the authority’s security policy. Any use of the data for purposes other than those of the authority or incompatible with those purposes could result in the Councillor acting ultra vires, breaching confidence or committing an offence under the Act.

Committee Meetings

Under the Local Government Act 2000 most authorities will be adopting new political structures although some smaller authorities will still have Committee systems. Even those authorities with new political structures will have committees for Planning, licensing and certain appeals.

Most committee agendas are divided into different parts with some parts to which the public have access and others which are held in private. Councillors are entitled to attend meetings of committees of which they are not members especially if they have a special interest in the items being discussed. In so doing they will receive the same items of information as members of the committee but are unable to participate in the discussions although in some cases they may speak. The information Councillors receive in order to enable them to follow the proceedings of the meeting must not be used for any other purpose unless authorised by the authority.

A Councillor requesting access to information about matters dealt with by a committee of which he/she is not a member must demonstrate a need to know. This is similar to the rules applying to employees of the authority when requesting access to data held by the authority for purposes other than those for which the employee normally processes personal data.

Meetings of the Executive

Under the new constitutional arrangements meetings of the Executive will be held in public if they are taking a key decision unless one of a certain number of exemptions apply.

The duties of Councillors involve them in acting on behalf of individual constituents or groups of constituents. Disclosure of personal data will be essential if they are to perform this function. Where the Councillor is merely passing on or investigating a complaint or series of complaints he/she will be regarded as a recipient of the data as described above. There will be occasions,
however when the Councillor will be acting on behalf of a constituent as agent or representative.

In such cases the Councillor is required to demonstrate that he/she is acting on behalf of the individual and has their consent for the personal data to be disclosed to the Councillor. This can be a copy of a letter received from a constituent.

**Confidential and Sensitive Information**

Although Councillors will appear on an authority's notified particulars and in information provided to data subjects as a group of recipients of personal data, there are certain categories that will not be automatically disclosed to the Councillor.

Information provided to the local authority in confidence. Such information is normally provided on the understanding that it will only be processed for the purpose for which it was provided and disclosed only to recipients with a need to know. Unless the Councillor has been identified as someone with a need to know (e.g. he/she is a member of a selection committee or social services case conference which has been provided with confidential information for use in its deliberations) such information will be withheld.

a) Information relating to the racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the health or sex life of an individual.
b) Information held by the police for the purposes of carrying out a criminal investigation.

Disclosure of the above categories of personal data will only be allowed where the following conditions have been satisfied.

a) Confidential information The Councillor has demonstrated a need to know, has the permission of the data subject or the provider has agreed to the disclosure. (see the note below)
b) Sensitive information where the data are required by Councillors in the decision making process and the data subject has consented to the disclosure for the process concerned. Where the disclosure concerns health data, it must only be disclosed if in the opinion of the appropriate health professional no harm will befall the data subject.
c) Police information Where disclosure of information will not prejudice any investigations. (e.g. information required for the eviction of or re-housing of nuisance tenants and sex offenders)

**NOTE:** Councillors might receive information in confidence when:

**Dealing with constituents:**

- making complaints especially against neighbours /other individuals
- providing personal details to enable the Councillor to act on his/her behalf
- reporting cases of anti-social behaviour - child abuse, abuse of the elderly etc.

**Acting on behalf of the council:**

- in order that he/she can represent the views of the council
• as part of joint initiatives with other public/private bodies

• as part of a case conference dealing with individuals.

To process such data for any other purpose may constitute unlawful processing within the meaning of the Act. Councillors should always be clear about the purpose(s) for which they have been given information and not use it for other purposes. This is especially important in instances where the need to act in the public interest could be considered to counter balance the duty of confidentiality.

In practice personal data collected by an Councillor for the purpose of investigating a complaint on behalf of a constituent should not be used for any other purpose neither should it be retained once the complaint has been effectively dealt with.

It is unlawful for any person to knowingly or recklessly obtain or disclose personal data without the consent of the data controller; this includes selling personal data obtained unlawfully. It is a defence if the person acted in the belief that he/she had a legal right to obtain or disclose the data, and that he would have had the approval of the authority, and that in particular circumstances his actions were justified as being in the public interest.
PART V – RIGHTS OF THE DATA SUBJECT

Councillors will also be data subjects and have new and improved rights in respect of personal data processed about them. The sixth data protection principle requires data controllers to process personal data in accordance with these rights.

The data subject’s rights are:

- The right of access
- The right to prevent processing likely to cause damage or distress
- The right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision-taking
- The right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

In order to deal with these rights, Councillors who are data controllers must:

- Provide the individual with information about the purposes for which he processes personal data, a description of the personal data held and a description of the recipients or classes of recipients to whom the data are or may be disclosed.

- Respond to the individual’s written request for access to personal data held about him/her. Upon payment of the fee (a data controller can charge up to £10) a copy of the personal data requested must be provided within 40 days. It is necessary to ensure the data provided do not reveal the identity of another third party individual and that information supplied by a third party is not revealed without first seeking the permission of the source.

- Respond to the data subject’s notices, requesting the Councillor to cease processing personal data for direct marketing or to cease processing if it can be proved that such processing is causing financial damage or distress.

- If you use automatic processes to reach decisions affecting the individual - in the conduct of his own business – comply with any notice from the subject requesting him to cease doing so. The controller is also required to provide the subject with details of the logic involved in any such processing.

- Establish procedures to correct personal data which the subject claims is incorrect or if the data have been provided by a third party source to retain the data provided by the subject together with the original data and make a note to the effect that the accuracy is in dispute and awaiting verification. The controller should also inform third parties to whom the personal have been disclosed that the data have been corrected etc.

Note: such action could obviate the need for the subject to take action through the courts to have data corrected, erased, destroyed or blocked.

The Act entitles a subject to compensation for damage by reason of any contravention of any of the requirements of the Act by a data controller. It is a defence for the controller to prove that he/she had taken all the care necessary to ensure compliance with the particular requirement.
Where a Councillor has received personal information from the LA to enable them to carry out their functions, as a member of the council and its committees, the Councillor is not required to respond to requests for subject access but must pass the request on to the appropriate person in the Local Authority. Councillors receiving such requests maybe required by the LA to provide it with any personal information held for the authority’s purposes.

Councillors who are unsure about what to do should contact the authority’s Data Protection Officer.
APPENDIX A

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   a) At least one of the conditions in Schedule 2 of the Data Protection Act is met, and
   b) In the case of sensitive personal data at least one of the conditions in Schedule 3 is also met. (See Appendix B)

2. Personal data 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. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall 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 this Act.

7. Appropriate technical and organizational 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 territory or country 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.
APPENDIX B

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing

2. The processing is necessary-
   a) for the performance of a contract to which the data subject is a party, or
   b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary
   a) for the administration of justice,
   b) for the exercise of any functions of either House of Parliament
   c) for the exercise of any functions conferred on any person by or under any enactment
   d) for the exercise of any functions of the Crown, a Minister of the Crown, or a government department, or
   e) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. The processing is necessary for the purpose of legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
CONDITIONS RELEVANT FOR THE PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

   (2) The Secretary of State may by order-

   - exclude to application of sub-paragraph (1) in such cases as may be specified, or

   - provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied

3. The processing is necessary in order to protect the vital interests of the data subject or another person, in a case where: consent cannot be given, by or on behalf of the data subject, or in order to protect the vital interests of the another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes and which is not established or conducted for profit; is carried out with appropriate safeguards for the rights and freedoms of data subjects; relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and does not involve disclosure to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps taken deliberately by the data subject.

6. The processing is necessary for the purpose or in connection with any legal proceedings (including prospective legal proceedings); is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. The processing is necessary for the administration of justice; for the exercise of any functions of either House of Parliament; for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

8. The processing is necessary for medical purposes and is undertaken by a health professional or a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional

9. The processing is of sensitive personal data consisting of information as racial or ethnic origin; is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained and is carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The processing is of sensitive personal data consisting of information as to the religious beliefs or other beliefs of a similar nature or of different states of physical or mental health or condition of the individual and is necessary for identifying or keeping under review the existence or absence the of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained.

11. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.
APPENDIX C.

LAWFUL PROCESSING

The first principle requires that personal data shall be processed fairly and lawfully. The principle further states that data are to be treated as obtained fairly if they consist of information obtained from a person who is authorized under or by any enactment to supply it or is required to supply it by or under any enactment or other convention or instrument imposing an international obligation on the UK. One of the conditions relevant for the purposes of compliance with the first principle is that the data controller is required to carry out the processing for compliance with a legal obligation to which he is subject.

The second principle states that data held only for one or more specified and lawful purposes shall not be further processed in any manner incompatible with these purposes. In interpreting this principle the Act further states that “in determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained regard is to be had for the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

In practice this implies that data controllers must ask third parties requesting access to or disclosure of personal data held by the controller, for his lawful purposes, for details of the purpose for which the third party intends using the personal data requested. The data controller must therefore determine whether the requestor’s purpose is compatible with his purposes or whether a disclosure to the third party would be a breach of the Data Protection Act and in particular the first and second principles.

Local authorities and Councillors dealing with such requests should examine any statutes governing their use(s) of personal data to discover if such data can be disclosed for any other purpose. Much of the law governing local authority use of data limits the use only to the purposes of the functions specified by the particular enactment. Additionally both should look at the information they provide data subjects regarding their reasons for holding the data and the purposes for which it was required.

A definition of the term ‘lawful’ does not appear in the Data Protection Act. It was, however, considered in a House of Lords case in 1991. In that case, ‘unlawful’ was held to mean:

"...something which is contrary to some law or enactment or is done without lawful justification or excuse."

This definition applies equally to breaches of statutory and common law. The effect of such a broad definition is that a data user must comply with all the relevant rules of law in relation to the purpose for which he or she holds personal data and the way in which such data is obtained and processed.

The doctrine of Ultra Vires is of relevance in this context. This is the rule of law limiting those vested with statutory powers to the performance of those things they are allowed to do by statute. Included in this is the doing of anything incidentally required to allow the fulfillment of primary functions. Any statutory body, inclusive of local authorities and their Councillors, which obtains, processes or holds personal data for a purpose for which it has no statutory authority could, therefore, be acting ultra vires and thus unlawfully in so doing.

Compliance with the Act, however, requires as one of its conditions that the data controller has obtained the data subject’s consent to the processing of the personal data. Such consent will be
necessary where the authority and/or an Councillor is processing or wishes to process personal data for any purpose not covered by a legal obligation imposed by statute or which does not meet any of the other conditions imposed by the first principle. **The Councillor should always ensure that both he and his authority have adequate statutory justification for their purposes. Where doubt exists the advice of the authority's legal advisors must always be sought.**

In the context of lawfulness it is necessary to consider also, that there are circumstances in which an obligation of confidence can arise between the provider of the information and the Councillor. In the context of Data Protection such an obligation gives the data subject the right not to have his/her information used for any other purpose or disclosed without his/her permission unless there are over-riding reasons for this to happen. Where such an obligation exists it may be unlawful for the Councillor to use the information for a purpose other than that for which it was originally provided.
APPENDIX D

DEFINITIONS

The following terms appear throughout the document and are defined here in order to assist the Councillor’s understanding of the key requirements of data protection.

Accessible record
An accessible record is a health record, consisting of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual.

Data
The Act refers to “data” as meaning information which –
   a) is processed by means of equipment operating automatically in response to instructions given for that purpose,
   b) is recorded with the intention that it should be processed by means of such equipment.
   c) is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system,
   d) forms part of an “accessible record” or,
   e) any recorded information held by a public authority (as defined in the Freedom of Information Act 2000)

note: the reference to information held by a public authority shall be construed in accordance with section 3(2) of the Freedom of Information Act 2000

Data Controller
A person who determines the purposes for which and the manner in which any personal data are, or are to be processed. The Councillors’ role as controller is discussed in the document.

Data Subject
The data subject is an individual, who is the subject of personal data. Constituents, complainants, Councillors, Council officers etc. may all be data subjects.

Subject Access
This is the right which each individual has to access personal data held about him/her by a data controller. The individual can exercise this right at any time, and is entitled to be informed by the controller whether personal data of which he is the subject are being processed and to be provided with a copy.

Personal Data
Means personal information that relate to a living individual who can be identified from that information and other information which may be in the possession of the data controller. Personal data includes expressions of opinion about the individual and any indication of the controller’s or any other person’s intentions regarding the individual.

Processing
Processing means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data or carrying out any operation or set of operations on the information or data. Such operations include organising the data, adapting it, altering it, retrieving it, consultation, use and disclosure by transmission, dissemination or otherwise making it available, of the data and operations such as alignment, combination, blocking erasure or destruction of the information or data.
**Recipient**
Any person to whom personal data are disclosed. This includes any person, such as an employee or agent of the data controller to whom they are disclosed in the course of processing the data for the data controller. The definition does not include any person to whom disclosure is made as a result of or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

**Relevant Filing System**
Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the is structured either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

**Unstructured personal data**
“Unstructured personal data” means any personal other than information which is recorded as part of or with the intention that it should form part of, any set of information relating to individuals or by reference to criteria relating to individuals.