



# DATA PROTECTION CODE OF PRACTICE



# ***CODE OF PRACTICE CONTENT***

|  | <b><u>Page</u></b> |
|--|--------------------|
| 1. Introduction  | 3                  |
| 2. Definitions   | 3                  |
| 3. Organisational Responsibilities                                       | 4                  |
| 4. Ashfield Homes Limited Data Protection Policy                         | 4                  |
| 5. Duty of Confidentiality   | 4                  |
| 6. The Data Protection Principles  | 4                  |
| 7. Data Protection Notification  | 5                  |
| 8. Renewal of the Notification   | 5                  |
| 9. Modification to Existing Data Processing                              | 5                  |
| 10. Implementation of New Data Processing                                | 5                  |
| 11. Responsibilities of Directors - Notification                         | 6                  |
| 12. Compliance with the Data Protection Principles                       | 6                  |
| 13. Fair Processing/permissions/clear why information required           | 6                  |
| 14. Review of Data   | 6                  |
| 15. Retention Periods  | 6                  |
| 16. Disposal Arrangements  | 6                  |
| 17. Requests for Disclosure of Information under the Data Protection Act | 7                  |
| 18. Other Requests under the Data Protection Act                         | 7                  |
| 19. Disclosure to Outside Agencies                                       | 7                  |
| 20. Crime and Taxation Disclosure  | 7                  |
| 21. Reference to Data Protection Officer or Legal Department             | 7                  |
| 22. Auditors   | 8                  |
| 23. CCTV Systems   | 8                  |
| 24. Ashfield Homes Limited Acting as Data Processor                      | 8                  |
| 25. Security of Manual Systems   | 8                  |
| 26. Secure Areas   | 8                  |
| 27. Prevention of Loss of Accidental Destruction of Data                 | 8                  |
| 28. Data Processors  | 8                  |
| 29. Internet and Email   | 9                  |
| 30. Employees  | 9                  |
| 31. Disciplinary Matters   | 9                  |
| 32. Staff Training/staff guide/induction training                        | 9                  |
| 33. Queries  | 9                  |
| <b>APPENDICES</b>  | <b>10</b>          |
| A. Ashfield Homes Limited Data Protection Policy Statement               | 11 - 12            |
| B. Procedure for responding to a Subject Access Request                  | 13 - 17            |
| C. Offences under the Data Protection Act 1998                           | 18                 |
| D. Staff Guidance on disclosure of personal information                  | 19 - 21            |
| E. Introduction to the Data Protection Act 1998 for Tenants              | 22 - 24            |
| F. ADC Councillor's Guide  | 25 - 48            |

# ASHFIELD HOMES LIMITED DATA PROTECTION CODE OF PRACTICE

## 1. Introduction

This Code of Practice refers to the Data Protection Act 1998, and supersedes the previous Code of Practice issued under the Data Protection Act, 1984. It should be read in conjunction with the Company's current Data Protection Policy Statement (Appendix A), and explains the way in which that Policy Statement shall be applied in order to comply with the requirements of the Data Protection Act 1998.

The purpose of the Code of Practice is to:

- ◆ Provide information to employees about the Data Protection Act 1998;
- ◆ Detail how the Company wishes the Act to be implemented
- ◆ Set out the procedures to be followed in specified circumstances

The requirements set out in this Code are of a general nature, and may need to be augmented by the more detailed instructions attached at Appendix B.

Periodic reviews of the Code of Practice will be carried out, and the Code amended in response to changing operational and legislative demands.

## 2. Definitions

Some of the definitions in the Data Protection Act, 1998, differ from those of the 1984 Act. For the purposes of implementation within this company, the following definitions are applicable:

|                        |  |
|------------------------|--|
| <b>DATA</b>            | Means information which <ul style="list-style-type: none"><li>◆ Is being processed by equipment operating automatically in response to instructions given for that purpose</li><li>◆ Is recorded with the intention that it should be processed by such equipment</li><li>◆ Is recorded as part of a relevant filing system or with the intention of forming part of such a system</li><li>◆ Forms part of an accessible record.</li></ul> <p>This covers not only computer records, but also relevant manual records containing personal data. The definition also covers CCTV, document image processing systems and audio material.</p> |
| <b>DATA CONTROLLER</b> | A "person" who (either alone or jointly or in common with other persons) determines the purposes and manner in which personal data are to be processed. The term replaces that of "Data User" in the 1984 Act. Ashfield Homes Limited is the Data Controller for the purposes of the Act.  |
| <b>DATA PROCESSOR</b>  | Means any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller. This broader term replaces the term "Computer Bureau" in the 1984 Act.   |
| <b>DATA SUBJECT</b>    | Means an individual who is the subject of personal data.   |
| <b>DISCLOSURE</b>      | Means disclosing the data to a third party (e.g. outside the company or to an employee or Board Member having no sufficient interest in the subject matter) the data, or information contained in the data.  |

**PERSONAL DATA**

Data consisting of information which relates to a living individual who can be identified from that data, or from other information in the Data Controller's possession, or likely to become so. It includes any 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.

**PROCESSING**

In relation to information or data, means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on it.

**RECIPIENT**

Any person to whom the data are disclosed (such as an agent or employee of the Company, a data processor or their agents or employees) including any person to whom they are disclosed in the course of processing. It does not include any person to whom the Company may be required by law to disclose in any particular case (e.g. by the Police under Warrant). It does include employees and agents of the Company.

**SENSITIVE PERSONAL DATA**

Means data consisting of information as to:

- ◆ Racial or ethnic origin
- ◆ Political opinions
- ◆ Religious or similar beliefs
- ◆ Whether member of a trade union
- ◆ Physical or mental health conditions
- ◆ Sexual life
- ◆ Offences or alleged offences
- ◆ Any proceedings for offences or alleged offences

**3. Organisation Responsibilities**

The Company's Data Protection Officer, with overall responsibility for Data Protection matters, is the Company Accountant/Secretary.

**4. Ashfield Homes Limited Data Protection Policy**

The basis for this Code of Practice is the Ashfield Homes Limited Data Protection Policy Statement, shown on Appendix A. This Code of Practice seeks to provide further guidance on the implementation of that policy. However, it is the Data Protection Act 1998, and any subsequent amendments, which are the definitive statement of the legal requirements.

**5. Duty of Confidentiality**

All personal data held by the Company is confidential. All persons having access to such data shall treat it as confidential, and shall disclose it only to the extent described in the Company's Notification or permitted by the Data Protection Act 1998.

**6. The Data Protection Principles**

Anyone processing personal data must comply with the "eight principles" of the Data Protection Act 1998.

The data must be:

1. obtained and processed fairly and lawfully and not processed unless certain conditions are met.
2. obtained for one or more specified and lawful purposes and not processed in any manner incompatible with those purposes.
3. adequate, relevant and not excessive.

4. accurate and up to date.
5. not kept for longer than is necessary.
6. processed in accordance with the data subject's rights.
7. kept safe from unauthorised or unlawful access/processing, and protected against accidental loss, destruction or damage.
8. not transferred to a country outside the EEA unless that country has equivalent levels of protection for personal data.

## 7. Data Protection Notification

The Data Protection Act 1998 replaces the previous registration regime with one requiring annual notification. The Information Commissioner maintains a Register of Data Controllers, which is based upon information notified by Data Controllers, and which is publicly available on the internet. The update of the Company's Notification will be undertaken by the Data Protection Officer.

Details of the Company's Notification are on the internet at:

[www.dpr.gov.uk/search.html](http://www.dpr.gov.uk/search.html)

Personal data may not be processed unless it is covered by the Company's Notification, or unless it is exempted by the Act from such notification.

Directors are responsible for identifying within their Departments systems which contain personal data, and for supplying the Data Protection Officer with the information necessary to ensure the processing is covered by the Company's Notification. If there is any doubt as to whether processing requires to be notified, the matter should be referred to the Data Protection Officer for determination.

## 8. Renewal of the Notification

The annual renewal of the Council's Notification will be undertaken by the Data Protection Officer.

Before expiry of the Company's annual Notification, the Data Protection Officer will request, in writing, the Directors to confirm that there have been no changes to the processing of their respective department which will require modification to the Company's Notification.

Where there are changes, these should be notified to the Data Protection officer with confirmation that all other relevant systems remain unchanged. The Data Protection Officer will advise where processing is being carried out which is not within the terms of the Company's Notification, and may request that processing be suspended until the statutory period of 28 days has elapsed in order to avoid unlawful processing.

## 9. Modification to Existing Data Processing

Where the manual or computerised systems involving the processing of personal data are modified, and such modification results in changes in processing which may not be covered by the Company's Notification, details should be passed to the Data Protection Officer before the revised processing commences.

If it is confirmed by the Data Protection Officer that revision to the Company's Notification is appropriate, 28 days must be allowed from the time the Information Commissioner is notified before commencing the revised proceedings. To process the data within this period could result in the commission of an offence.

## 10. Implementation of New Data Processing

All new manual or computerised systems involving the use of personal data must comply with the Company's Notification. Directors should ensure that the processing is covered by the Company's registration before the new system is implemented.

Where the new system is not covered by the Notification, or there is reason to believe this is to be the case, details should be passed to the Data Protection Officer for action. The system should not be implemented.

If the system is determined to be covered by the Notification, it may be implemented without further delay.

If however, it is confirmed by the Data Protection Officer that revision to the Company's Notification is appropriate, 28 days must be allowed from the time the Information Commissioner is notified before commencing the revised proceedings.

#### **11. Responsibilities of Directors – Notification**

Directors must ensure that operational manual and computerised systems and records comply at all times with the Company's Notification, and ensure that any changes thereto are dealt with in accordance with this code, and with the requirements of the Data protection Act 1998.

#### **12. Responsibilities of Directors – Data Protection Principles**

Directors should ensure that:

- ◆ all processing within their Departments are carried in accordance with the Data Protection principles, and with the "fair processing" requirements of the Act;
- ◆ all staff are aware of their obligations under the Data Protection Act 1998;
- ◆ new staff are made aware of these obligations as part of their training.

#### **13. Fair Processing/permissions/clear why information required**

All requests for information issued by the Company shall, where it is deemed necessary, specify the purposes for which the information is required, and to whom the information is to be disclosed. Directors should take action to review such documentation, to ensure that it complies with this requirement.

#### **14. Review of Data**

The Act requires that reasonable steps are taken to ensure that data is accurate and up to date. Directors should ensure, where necessary that review procedures are in place to update personal information, and verify its accuracy. In addition, the Act requires that personal data shall be "adequate relevant and not excessive" to the purposes for which it is obtained.

Such procedures should be documented, and all Managers made aware of them.

#### **15. Retention Periods**

According to the Act, personal data should not be kept longer than is necessary, although it does not specify how long a period this should be.

Directors should be satisfied that there is a specified retention period for all their systems containing personal data, and that there are arrangements to remove obsolete records at the end of these periods.

Such procedures should be documented.

#### **16. Disposal Arrangements**

The Act requires that personal data should be kept safe from unlawful and unauthorised processing, and secure against accidental loss, destruction or damage.

Directors should therefore ensure that there are arrangements in place for the disposal of personal data when it is no longer required, and that all staff dealing with the data are aware of the arrangements.

The procedure should be documented.

#### **17. Requests for Disclosure of Information under the Data Protection Act**

The Data Protection Subject Access Procedure, which is contained in Appendix B to this Code of Practice, should be followed in all cases where such a request is received.

Written disclosure of personal information in response to a data subject access request will be made only by the Data Protection Officer.

#### **18. Other Requests under the Data Protection Act**

Under the Data Protection Act 1998 a data subject has the right to serve written notice requiring the Company.

- ◆ To cease, or not to begin, processing their personal data where such processing is likely to cause damage or distress;
- ◆ To cease, or not to begin, processing their personal data for the purposes of direct marketing;
- ◆ To ensure that no decision which significantly affects the data subject is based solely on processing their personal data by automatic means.

Any such written requests should be referred to the Data Protection Officer without delay.

#### **19. Disclosure to Outside Agencies**

Disclosure of personal data to outside agencies such as credit agencies, banks, building societies etc. may be made even if such disclosures are not notified, provided that the data subject has requested, or has given consent to, such disclosure.

Normally, such a request should be in writing and should contain a signed declaration by the data subject consenting to the disclosure.

If the request does not come directly from the data subject, the relevant agency must provide documentary evidence of such approval before any information is released.

With regard to Company employees, no personal data will be disclosed until that person has given his/her written approval, or a consent form has been signed with the agency concerned.

#### **20. Crime and Taxation Disclosure**

Personal data may be disclosed without authority of the data subject if disclosure is:

- ◆ For the prevention or detection of crime;
- ◆ For the apprehension or prosecution of offenders;
- ◆ For the assessment or collection of any tax or duty or of any imposition of a similar nature;
- ◆ Where non-disclosure might prejudice the foregoing;
- ◆ Where disclosure is required by or under any enactment, by any rule of law or order of the court;
- ◆ Where disclosure is necessary for or in connection with any legal proceedings or for the purposes of obtaining legal advice, or is necessary for establishing, exercising or defending legal rights.

#### **21. Reference to Data Protection or Legal Department**

Where a Court Order is received requesting disclosure of personal information it should be referred to the Company's Solicitor without delay. If valid, the information must be disclosed according to the order.

Requests for disclosure under the categories cited at 21 above which are not supported by Court Order should be referred to the Data Protection Officer to ensure that disclosure is permissible. In the opinion of the Information Commissioner, for a requestee simply to cite one of the above categories is not, in itself, sufficient justification for the personal data to be released.

## 22. Auditors

An Internal auditor of the Company shall have access to any records or documents of the Company for the purposes of internal audit. In addition, an auditor shall have disclosed to him/her from any officer of the Company any information or explanation of information that is necessary for the purposes of audit.

The same access will be afforded to external auditors authorised to examine the Company's accounts.

## 23. CCTV Systems

Operation of any CCTV systems shall be in accordance with the requirements of the Data Protection Act 1998, and conform to guidance issues from time to time by the Information Commissioner. Where required, copies of this guidance can be obtained from the Data Protection Officer.

## 24. Company Acting as Data Processor

Where the Company acts as Data Processor for other organisations, it is the responsibility of the relevant Data Controller to ensure and regulate compliance with the Data Protection Act 1998.

## 25. Security of Manual Systems

All manual systems/records containing personal data should be securely stored, and measures taken to ensure the reliability and awareness of staff having access to it. Transmission of personal data between locations should accorded the same level of security.

Only those authorised to do so may process personal data. Waste materials must be disposed of in accordance with security procedures, and with due regard to the sensitivity of the data, and the harm which could result from unauthorised use.

Directors should ensure that appropriate security and secure disposal arrangements are in place.

## 26. Secure Areas

Only authorised persons should be allowed into secure areas. Access should be by key, identity card, access token or access code and these should not be given or disclosed to unauthorised staff.

The loss of such items must be reported to the Director as soon as it is discovered.

## 27. Prevention of Loss or Accidental Destruction of Data

The Company's policy regarding the security of IT systems, access and security restrictions as well as the back-up procedures to guard against the accidental loss or destruction of data, is contained on its "IT Security Policy". Directors should ensure that the requirements of the policy are complied with, and that all staff are aware of them.

## 1 Data Processors

The Act states that where processing of personal data is carried out by a Data Processor then the Data Controller must:

- ◆ Choose a Data Processor providing sufficient guarantees in respect of technical and organisational security measures governing the process to be carried out;
- ◆ Take reasonable steps to ensure compliance with these measures, and;

Controlled document –

8

Changes to be made by Company Secretary only

Latest version 27/4/05

Formatted: Bullets and Numbering

Deleted: 16/9/04

- ◆ The processing must be carried out under a contract which is in writing and
- ◆ Under which the Data Processor is to act only on instructions from the Data Controller, and
- ◆ The contract requires the Data Processor to comply with obligations equivalent to those imposed on the Data Controller.

*(Data Protection Act 1998; Schedule 1, Part II, 10-11)*

It is the responsibility of Directors to ensure that their Data Processors are so regulated, and to notify the Data Protection Officer of such situations.

### **29. Internet and Email**

The Company permits access to the Internet, and to e-mail facilities only under the conditions laid down in the relevant policy documents.

### **30. Employees**

Directors should ensure that all employees having access to personal data and aware of their Data Protection Act responsibilities, and have the level and degree of access to the personal data appropriate to their job.

### **31. Disciplinary Matters**

Company employees who deliberately or recklessly disregarded the Data Protection Act 1998, the Company's Data protection Policy Statement and/or Code of Practice will be dealt with under the Company's normal disciplinary procedure.

### **32. Staff Training**

Personnel Department will notify all new members of staff of the general requirements of the Data Protection Act 1998 by inclusion of the Data Protection Staff Guide in their induction information pack.

### **33. Options**

The Data Protection Officer has overall responsibility for advising the Company and its employees on the Data Protection Act 1998, and for ensuring the Company's compliance with its provisions.

Queries relating to the Data Protection Act 1998, the Company's Data Protection Policy Statement, or Code of Practice should be raised with an immediate supervisor or the Data Protection Officer.

# APPENDICES

Controlled document –  
Changes to be made by Company Secretary only  
| Latest version [27/4/05](#)

10

Deleted: 16/9/04

# **APPENDIX A**

## **Ashfield Homes Limited Data Protection Policy**

### **DATA PROTECTION POLICY STATEMENT**

1. Ashfield Homes Limited fully supports the objectives of the Data Protection Act 1998.
2. The Act requires the Company, as a data controller, to notify the Information Commissioner of the data subjects, the classes of data being processed, and to whom the data will be disclosed. The Company affirms its policy of complying with the notification requirements of the Act, and of maintaining that compliance. Failure to notify-is a criminal offence.
3. The Company reaffirms its present policy of maintaining the confidentiality of personal information held in its computerised and manual records, and expects all its employees and board members to comply fully with the Data Protection Code of Practice and the Principles of the Data Protection Act.
4. All staff must be aware of the Data Protection Act, and of their obligations under it. Individual staff and board members may be personally liable for breaches of the act if they act outside their authority.
5. All new members of staff will receive information about the Data Protection Act as part of their Induction Process.
6. The Company will hold no more personal information than is necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. The Company will seek to ensure that information is accurate, up-to-date, and that inaccuracies are corrected without unnecessary delay.
7. Personal data must be treated as confidential. Sources and disclosure of personal data must be in accordance with the provision of the Data Protection Act, and the Company's registration under it. Therefore personal information will be disclosed, for registered purposes only, to; data subjects, bona fide agents of the data subject, others as detailed in the registration, and, for other purposes, only to the Courts (under the direction of a Court order), the Police in the investigation of crime or at the request or with the consent of the data subject.
8. All Data Subject Access Requests for information made to the Company under the Data Protection Act 1998 will be dealt with by the designated officers, and in accordance with the Company's Data Protection Code of Practice.
9. The maintenance of the Company's compliance, annual renewal of registration, dissemination of data protection information within the Company and dealing with changes and modifications arising from legislation or codes of practice, is the responsibility of the designated officers.
10. It is the responsibility of Heads of Service to ensure compliance with this policy within their own Services. All systems, both computerised and manual, which contain information about individuals, must comply with the requirements of the Data Protection Act 1998 and be dealt with in accordance with the Company's Data Protection Code of Practice. For registration purposes the designated officers must be notified of the details of these systems and of any known future developments likely to affect registration.
11. In addition it is the responsibility of Heads of Service to ensure that any new computerised or manual systems are compliant with the Data Protection Act.
12. Access will be afforded in accordance with the Act to data subjects applying for such information in the specified manner, for which a fee of £10 + VAT will be charged. No fee, however, will be charged to employees or board members for information relating to their employment or duties.
13. In cases where the Company acts as a data processor, that is as a bureau providing computer services to outside organisations:

(a) no disclosure will be made without the written instruction of the data controller except under the direction of a Court Order, and

| ( ) as specified in the Data Protection Act 1998, the Company will undertake only such processing as is contractually agreed with the data controller.

| 0. The Company expressly prohibits the use of the Company's computing equipment and/or software for any unauthorised purposes. Authority for uses unconnected with the Company's responsibilities and functions may be given by the Chief Executive or by the Data Protection Officer.

| 0. Disciplinary action may be taken in the case of any Company employee breaching any instruction contained in, or following from, this Data Protection Policy.

# APPENDIX B

## Guidance notes for responding to a Subject Access Request

### Step 1 – Receiving a valid request

The Data Protection Act 1998 gives all individuals the right to see and obtain a copy of any information that is held about them by others. The right applies to anyone about whom Ashfield Homes Limited holds information. This could be staff, ex-staff, residents, tenants, service users, suppliers, contractors. Therefore, if the Company holds data on individuals or companies, if the subject of the data so requests, the Company is required to provide details of the data held. To exercise this right, individuals or companies make what is known as a subject access request. That is, they make a request for information where they are the subject of that information or data. The Company is legally obliged to respond to requests within 40 calendar days. To fail to do so is a breach of the Act and could lead to a complaint to the Commissioner (formerly the Data Protection Commissioner).

Below is a procedure to assist staff to respond to a request from an individual for information that the organisation holds about them.

**For a request to be a valid request under the Act, it needs to be in writing. A request by email can be accepted.**

If someone comes into the offices or if we receive a telephone request for personal data, we should ask the individual to put their request in writing. A form has been developed to assist individuals with their request. However, using the form is not a requirement, as long as the data subject's request is in writing, and contains the information we reasonably require in order to comply with it, we must respond to it.

***Pass the request to Administration at Head Office***

### Fees

***The organisation is permitted to charge a fee of up to £10 for each Subject Access Request. The person making the Subject Access Request should be advised of this charge at the time of their request and payment of the fee should accompany the request.***

Deleted: + VAT

### Step 2 – Recording the request

It is important that we keep a record of our handling of the request from the moment it is received to when it is finalised. On receipt of the proper written request, the Administration Department will record the date of the request and enter it into a separate manual file for subject access requests, keeping copies of all correspondence, notes made, summary of phone conversations, dates received and actioned. A deadline of 40 calendar days has been set down in law by which we have to have responded to the request.

***The 40 day deadline***

The deadline set down in the law is 40 calendar days. The Act makes no allowances for holiday periods or public holidays. It is therefore important that Managers take responsibility for ensuring any subject access request is given priority.

The 40 days starts from either:

1. the date of the receipt of the written request if we have everything you need to proceed with the request; or
2. the date on which we receive the information that you need to:
  - a) clarify the request in order to locate the data; and/or
  - b) satisfy ourselves of the person's identity.

Once we have calculated the start date, add the 40 day deadline to the record. **In the acknowledgement letter, it is important that we explain to the individual the date upon which the request must be completed.**

## **Step 3 – Acknowledging, clarifying and verifying the request**

### ***Making contact with the individual***

It is often helpful to make contact with the individual as soon as the request is received to establish exactly what information he or she seeking. Even if their request is a general one, in some cases individuals may actually be seeking specific information. The Administration Department will send the data subject a standard letter of acknowledgement within seven days of the written request, and if where necessary make telephone contact with the individual. Administration will record the date of the acknowledgement letter and the date and outcome of any telephone contact made. Additionally they will record the verification steps taken and make note of any relevant documents that have been seen.

***The administration section will then pass the request on to the manager(s) of the appropriate department in order to search for the requested data.***

The right of subject access applies whatever the motive of the data subject for seeking the information. We are not permitted to ask the data subject why they are seeking the information. Even where the individual tells us about their intention to use the data, for example for legal action, this does not entitle us to refuse.

### ***Requests made on behalf of the individual***

Another person may also make a request on behalf of the individual, for example, a solicitor or a family member. Care must be taken to ensure that we are satisfied that the individual has given their authority. For example we could ask to see a copy of a Power of Attorney or a document signed by the individual giving their authorisation.

### ***Verifying the identity of the individual***

We are entitled to ask for any information that we may reasonably require to satisfy ourselves of the identity of the individual. What you ask for must be appropriate for our work area and proportionate to the nature of the information sought. For example, if it involves sensitive information we would expect to require more proof of identity. Some examples include:

- driving licence;
- birth certificate;
- passport;
- rent book;
- recent utilities bill;

- customer or user number

It may not be necessary to retain copies of documents but a record must be kept that we have signed the appropriate documents to verify the identity of the individual.

## **Step 4 – Finding and checking the requested information**

***PLEASE NOTE THAT NO AMENDMENTS OR ALTERATIONS, OTHER THAN THOSE WHICH WOULD HAVE BEEN MADE IN THE NORMAL COURSE OF EVENTS, MAY BE MADE TO THE RELEVANT RECORDS ONCE THE SUBJECT ACCESS REQUEST HAS BEEN RECEIVED.***

The appropriate manager(s) will search for the requested data on the relevant databases or paper based systems.

### ***What we must provide***

The following types of record come under the Act and must be provided should an individual request them. Again, it is important to narrow down the search as much as possible, particularly if it involves searching for various types of records and over a range of time periods.

Information in electronic form:

- computerised records on database;
- images or documents on computerised systems;
- emails;
- CCTV

Manual files must be made available after 24 October 2001. These files fall under the Act if they are in a filing system that is structured by reference to the individual or in some other way that allows an individual's information to be easily accessible.

Backup data also falls under the Act. However, a search should only be conducted if specifically asked for.

### ***What we do NOT have to provide.***

There are some types of information which the Act says we do not have to provide when an individual makes a subject access request. These are summarised below and should be dealt with on a case by case basis. It is recommended that any decision to withhold information is handled by the Company Secretary/Accountant of before deciding to withhold any information.

We are permitted to withhold the following:

- Information that is likely to prejudice any of the following purposes:
  - prevention or detection of crime;
  - the apprehension or prosecution of offenders;
  - the assessment or collection of any tax or duty
- Confidential references given by a staff member to a prospective employer.
- Certain records relating to health, education and social work.
- Any records of the intentions of the organisation in negotiations with the data subject.

- Information which is subject to legal professional privilege.
- Information that would lead to self incrimination.

Ensure that we record any information that we have decided to withhold, noting which exemption we are relying on.

***Where the requested information identifies other people.***

Where the requested information includes personal data on another individual (a third party), we need to consider whether to release that information to the data subject. There are three actions we can take.

- Edit the information so as not to reveal the third party’s identity, for example, blocking out the text or re-typing text without the identifying information; or
- Obtain the third party’s consent to the disclosure, if it is reasonable to do so; or
- Decide whether that it is reasonable to disclose the information to the data subject without the third party’s consent.

In taking this third option we need to consider:

- whether you owe the third party the duty of confidence;
- what steps taken to get their permission;
- whether the person is capable of giving consent;
- whether he/she has expressly refused consent;
- whether the information is of particular importance to the data subject.

The European Court of Human Rights has ruled that in certain circumstances the individual's right of access to information is so important that their rights override the third party's rights to confidentiality.

## **Step 5 – Preparing to release the information**

The appropriate manager prepares a letter to accompany the information intended for release ensuring that you add your contact details so that the data subject can advise you whether he or she thinks that the information is inaccurate or incomplete. Copy all this to the Administration Department so that they can log the date sent against the original application.

We are required to provide the individual with an intelligible copy of the data in permanent form, for example photocopy or print out. We may provide the data in other forms if the individual agrees with this or specifically requests it. We may be able to decline to provide a copy of personal data in permanent form if it would require “disproportionate effort”, for example, if the printed version has to be retrieved from a remote archive. This doesn’t mean that we can withhold the requested information in its entirety, simply that we do not have to provide the data in permanent form. You must still offer to supply the data in another form.

**To make the information intelligible we must, for example, explain any special codes you use either in the document containing the information or in a separate explanatory leaflet.**

## **Step 6 – Responding where no information has been found**

If no information has been found, send a letter to the data subject indicating this or, if none of the data can be released, state that there is no information you are required to give. There is no requirement to explain the reason for withholding. Copy to Ashfield Homes Limited Administration Department who will log date sent with original application.

## **Step 7 – Finalising the request**

It is important that we retain records of your final response to the individual – identifying any information that was sent should the individual challenge what was provided/not provided. Individuals have rights to have any inaccurate information corrected. They can also request that we discontinue processing where it causes them damage or distress. If you receive such a complaint you are required by law to:

- Respond within 21 days to the data subject;
- Advise them whether it is appropriate for you to change any data or cease any processing;
- Give them the reasons for the decisions.

If the individual disputes your decision, he or she can lodge a complaint with the Commissioner.

Keep all documentation on a file for a maximum of two years in case any further action is required.

## **Frequency of Data Subject Access Requests**

The Data Protection Act permits the data controller to refuse to meet requests to access an individual's records that are made too frequently. This is a provision to safeguard data controllers from vexatious requests.

It is the Company's intention not to comply with requests made more often than twice a year, and a 3 month interval should have elapsed since the previous request. If requests are received more frequently than this, consideration should be given to any special circumstances which may make meeting the request desirable.

### **MANAGERS AND OFFICERS OF ASHFIELD HOMES LIMITED AUTHORISED TO DEAL WITH REQUESTS FOR PERSONAL INFORMATION**

Chief Executive Officer  
Director of Housing Services  
Assistant Director of Housing Services  
Director of Technical Services  
Assistant Director of Technical Services  
District Housing Manager  
Responsive Repairs Manager  
Support Services Manager  
Voids and Estates Manager  
Procurement Manager  
Company Accountant/Secretary  
Human Resource and Development Manager

**APPENDIX C**  
**Offences under the Data Protection Act 1998**

- ◆ Processing personal data without notification
- ◆ Failure to notify the commissioner of changes to the notification register entry
- ◆ Processing before expiry of assessable processing time limits or receipt of assessable processing notice within such time.
- ◆ Failure to comply with a written request for particulars.
- ◆ Failure to comply with an enforcement notice/information notice/special information notice.
- ◆ Knowingly or recklessly making a false statement in compliance with an information notice or special information notice.
- ◆ Intentional obstruction of, or failure to give reasonable assistance in, the execution of a warrant.
- ◆ Without the consent of the data controller, knowingly or recklessly to
  - Obtain or disclose personal data, or the information contained in personal data, or
  - Procure the disclosure to another person of the information contained in personal data, or transfer data, other than as described in the notification form (with certain exceptions)
- ◆ To sell or offer to sell personal data obtained in contravention of the “unlawful obtaining” prohibitions
- ◆ To sell or offer to sell personal data subsequently obtained in contravention of the “unlawful obtaining” prohibitions
- ◆ Enforced subject access

← --- **Formatted:** Indent: Left: 0.63 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm, Tabs: 1.27 cm, List tab + Not at 0.63 cm

**Conviction could lead to a fine at present not exceeding £5,000 if tried in a Magistrates Court, or an unlimited fine in the Crown Court.**

## APPENDIX D

### ASHFIELD HOMES LIMITED

#### DATA PROTECTION

#### STAFF GUIDANCE DISCLOSURE OF PERSONAL INFORMATION

##### 1. INTRODUCTION

- 1.1 The purpose of this guidance Note is to set out for staff the restrictions governing the disclosure of personal information, both to Board Members and officers of Ashfield Homes Limited and to Elected Members and Officers of Ashfield District Council.
- 1.2 This document should be read in conjunction with the **Ashfield Homes Limited Code of Practice** which sets out the requirements of the Data Protection Act 1998 and the methods by which Ashfield Homes limited intends to comply with them.
- 1.3 Staff dealing with personal data should be aware of the requirements of the Data Protection Act 1998, and be familiar with the contents of the **Ashfield Homes Limited Staff Guide**.
- 1.4 Ashfield Homes Limited acts in the capacity of an agent of Ashfield District Council with respect to managing Council tenancies and administering Council housing stock on the Council's behalf. The tenancy agreements are between the tenant and the Council, whilst the housing stock remains the property of the Council.
- 1.5 In carrying out its legitimate functions through the agency of Ashfield Homes Limited, Ashfield District Council is entitled to be furnished with relevant personal information relating to it's tenancies, subject to certain restrictions, which are dealt with in the following sections.

##### 2. TERMINOLOGY

- 2.1 The term "authorised manager or officer of the company" in this document means one of the posts listed in the attached Appendix 1.

##### 3. ADMINISTRATIVE ARRANGEMENTS

- 3.1 The Data Protection Officer for Ashfield Homes Limited is the **Company Accountant/Secretary** to whom any queries or requests for information should be addressed.

##### 4. DATA SUBJECT ACCESS REQUESTS

- 4.1 Data Subject Access Requests should be in writing, and should be referred to the Data Protection Officer immediately for action as per Ashfield Homes Limited's **Code of Practice**.

##### 5. DISCLOSURE OF PERSONAL INFORMATION

- 5.1 Disclosure of personal information by staff of Ashfield Homes Limited should be in accordance with:

- The Data Protection Act 1998 (including Subject Access Requests);
- [The organisation's Notification to the Information Commissioner](#), and

**Formatted:** Indent: Left: 1.24 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**Formatted:** Indent: Left: 1.24 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm, Tabs: 2 cm, List tab + Not at 2.54 cm

**Deleted:** AHL Code of Practice2.doc

- The agreement between Ashfield Homes Limited and Ashfield District Council regulating data processing.

**Formatted:** Indent: Left: 1.24 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

5.2 However, the following types of disclosures require some clarification:

- Disclosure to Ashfield Homes Limited Board Members
- Disclosure to Ashfield District Council Councillors
- Disclosure to Officers of Ashfield District Council

## 6. REQUESTS FOR PERSONAL INFORMATION – GENERAL PROCEDURE

**6.1 All requests for personal information, whether by Members of the Board of Ashfield Homes Limited, Members of Ashfield District Council, or Officers of Ashfield District Council must be made to an authorised manager or officer of the Company.**

6.2 If other officers of Ashfield Homes Limited receive such a request, it should be referred immediately to an authorised manager or officer of the company.

6.3 Each request should be in writing and the consent of the data subject to the release of the information should be provided.

## 7. DISCLOSURE TO ASHFIELD HOMES LIMITED BOARD MEMBERS

7.1 Board Members are entitled to the information necessary for them to be able to carry out their functions and it is unlikely that a tenant's personal details would normally be included.

7.2 All Board Members have signed an undertaking that any personal information to which they have access will be treated as confidential, and will be processed in accordance with the requirements of the Data Protection Act 1998.

## 8. DISCLOSURE TO ASHFIELD DISTRICT COUNCIL COUNCILLORS

8.1 Ashfield District Council Councillors may act in one of four capacities when requesting information:

- as Member of the Council (e.g. as a member of a Council Committee);
- as a representative of a resident of his/her ward (e.g. in pursuing a complaint);
- representing a political party (e.g. at election time); or
- as a Board Member of Ashfield Homes Limited

**Formatted:** Font color: Red

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold, Font color: Auto

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold

**Formatted:** Font color: Auto

**Formatted:** Indent: First line: 0 cm

**Formatted:** Bulleted + Level: 1 + Aligned at: 1.27 cm + Tab after: 2.54 cm + Indent at: 2.54 cm

**Formatted:** Indent: Left: 0 cm, First line: 0 cm

**Formatted:** Indent: Left: 2.54 cm, First line: 0 cm

**Deleted:** Member is entitled to the information necessary to carry out his/her duties, and this would not include access to tenants' personal details.

**Formatted:** Font color: Red

**Formatted:** Indent: First line: 0 cm

**Deleted:** AHL Code of Practice2.doc

8.2 As an Elected Member of the Council

There are three considerations when giving out information to Elected Members of the Council:

- The Member should only be given access to as much information as it is necessary to carry out his/her legitimate duties;

The purpose for which the information may be used or disclosed should be specified by the Elected Member, and a note made on an Elected Members Information Disclosure Register for recording purposes; and

Where the Elected Member is able to take a copy of the information away from AHL premises, the steps taken to ensure the security of the information should be specified to the Elected Member and recorded.

### 8.3 As a Representative of a Resident

Formatted: Font: Not Bold

Personal information may always be disclosed at the request of, or with the consent of the data subject.

Formatted: Font: Not Bold, Font color: Auto

Personal information may also be given to an Elected Member where he/she represents the ward in which the data subject lives (in which case there may be a reasonable presumption that the Elected Member is acting on behalf of the data subject. In other cases, or where the data in question is of a particularly sensitive kind, it may be prudent to seek the signed consent of the data subject.

Formatted: Font color: Auto

Formatted: Indent: First line: 0 cm

When providing information to an Elected Member it should be made clear that the information is provided for the limited purpose of assisting the data subject and that the information must not be used for any other purpose.

The Elected Members Information Disclosure Register should be completed on each occasion that information is disclosed to a member recording the requests made by Elected Members for information.

Deleted: , provided that the subject lives in the Councillor's area, and proof of their authority to so act is provided.

### 8.4 For Political Purposes

Formatted: Font: Not Bold

Staff should not disclose information to Elected members if it is clear that the information is required for political purposes.

## 1.1 As a Board Member of Ashfield Homes Limited

Formatted: Bullets and Numbering

Board Members are entitled to the information necessary for them to be able to carry out their functions and it is unlikely that a tenant's personal details would normally be included.

## 9. DISCLOSURE TO OFFICERS OF ASHFIELD DISTRICT COUNCIL

9.1 Disclosure to departments of the Council will be made in accordance with Ashfield Homes Limited "Notification to the Information Commissioner". Providing that the request for information from the Council department is in exercise of the Council's legitimate activity the requested information may be disclosed.

9.2 The request must be made in writing to the appropriate authorised manager or officer of the company giving the reason for the request.

1.1 If the purpose of the request is unrelated to housing issues then staff should refer to their manager.

Formatted: Bullets and Numbering

## APPENDIX

### MANAGERS AND OFFICERS OF ASHFIELD HOMES LIMITED AUTHORISED TO DEAL WITH REQUESTS FOR PERSONAL INFORMATION

Chief Executive Officer  
Director of Housing Services  
Assistant Director of Housing Services  
Director of Technical Services  
Assistant Director of Technical Services

Deleted: AHL Code of Practice2.doc

District Housing Manager  
Responsive Repairs Manager  
Support Services Manager  
Voids and Estates Manager  
Procurement Manager  
Company Accountant/Secretary  
Human Resource and Development Manager



**APPENDIX E  
INTRODUCTION FOR TENANTS  
TO  
THE DATA PROTECTION ACT 1998  
PERSONAL INFORMATION  
(YOUR RIGHT TO KNOW)**

**What is the Data Protection Act 1998?**

It is a new law which came into force at the end of October, 1998. It was introduced to protect personal data, that is data about individuals (you and me) no matter how it is processed, what it is processed for, or who processes it.

**How does it protect personal data about you?**

By setting rules and conditions which all users of personal information such as this Company (the Act calls us Controllers) must obey when obtaining and using information about you. The Act also provides you with certain rights which the controllers must respect.

**What are your rights?**

- To ask the Company if it holds personal information about you.
- To ask what it uses the information for.
- To be given a copy of the information.
- To be given details about the purposes for which the Company uses the information and of other organisations or persons to whom it is disclosed.
- To ask for incorrect data to be corrected.
- To ask the Company not to use personal information about you for direct marketing; which is likely to cause damage or distress or to make decisions about you based on the automatic processing of the data.
- To compensate for damage or distress should these be caused by our failure to comply with certain requirements of the Act.

**Why do we keep personal information?**

So that we can provide you with the services you require, collect rent, etc. and maintain a record of the services provided.

## **What services does the Company provide?**

- Tenant applications and lettings.
- Repairs service.
- Tenancy support.
- Collection of rent arrears

Does Ashfield Homes Limited need your consent to use information about you for any of these purposes?

We require your consent only if we are going to process data about you for purposes other than those we are required to provide by law, or where we intend using data required for one legal purpose for another. All application forms and requests for information explain why we require the information requested and whether or not we need your consent.

## **How do you ask to see information about you?**

You must write to the Company, to the address at the end of this leaflet, using the attached form asking to see your records. You will need to provide your name and address, details of the service(s) you are receiving and any other information (e.g. date of birth, rent or council tax number) that could help the Company find your information. If you call at any of the Company's offices, you will be given a copy of the 'Subject Access Request Form'. Help is available with filling in this form should you need it.

The request form will also be sent to you if you have not provided the Company with enough information.

## **Do you have to pay to see your information?**

Yes. A fee of £10 + VAT will be charged for each subject access request.

## **What information will you receive?**

All of the information Ashfield Homes Limited holds about you on both its computer and manual records, a description of the purposes for which we process your data, a list of others to whom it is disclosed and information about sources.

## **How will you be given the information?**

You will be given a copy to keep and check for accuracy. This will either be a printout from the computer or a photocopy of your manual records.

The Company can only disclose information to you relating to another individual if that person has consented to it, or it is reasonable, given all circumstances to disclose it.

## **What do you do if the data are incorrect?**

You must write to Ashfield Homes Limited telling it what data is incorrect and asking for the data to be corrected. The Company must tell you what it has done within 21 days of receiving your request. If the Company does not agree that the information is incorrect you can ask it to record your disagreement on your records. You can also appeal to the Information Commissioner or the court if the Company does not correct the information.

What do you do if you think you have not been given all of the information you asked for?

You can appeal to the Company through its appeals procedure or you can appeal to the Information Commissioner. The Commissioner's staff will look into the matter on your behalf.

**Deleted:** AHL Code of Practice2.doc

**How can you prevent the Company from using information about you for Direct Marketing or stop it from using information for a purpose which could cause you damage or distress?**

You should write to the Company asking it not to process your information for the first of these. If you think that the use could cause you damage or distress you must also write to the Company this time giving your reasons for asking them to stop the processing.

**How will you know if the Company has done as you asked?**

The Act requires us to respond no later than 21 days after we have received your request. If we do not do so or refuse to do as you ask you can appeal to the court.

**How will you know if decisions about you have been made by automatic means?**

We will tell you and ask you to write if you have any objections. If you do object the Company will make a new decision but this time will not do so by automated means.

**What can you claim compensation for?**

If Ashfield Homes Limited has broken any of the rules or conditions established by the Act and you have suffered damage or distress you may be able to claim compensation. You may also be able to claim compensation if the damage or distress was caused by our use of inaccurate data.

**How do you make a claim for compensation?**

Claims are made through the court which will only support these if you can show that the Company had not taken reasonable care to ensure it complied with the Act, and in the case of the use of inaccurate data, it is satisfied that you have suffered damage as a result of our use of such data.

**Does Ashfield Homes Limited provide help in understanding the information?**

Yes. If you need help with the information provided, the application form on this leaflet, if you let us know we will provide someone to assist you. A translation service is also available.

**Exemptions from the right to see your data**

There are a number of exemptions to your right to see information held about you. You will not be able to see information held for the purpose of:-

- Preventing or detecting crime
- Catching or prosecuting offenders
- Assessing or collecting duty or tax

**Address to which requests for access should be sent:**

The Company Accountant/Secretary  
Ashfield Homes Limited  
Head Office  
Innovate Office  
Willow Drive  
Sherwood Park  
Annesley  
Nottingham NG15 0DP

## APPENDIX F

### DATA PROTECTION: A COUNCILLOR' S GUIDE

#### Revised Guidance on the Implications of the Data Protection Act 1998 for Councillors





## **PREFACE**

The guide and the briefing note have been written by the IDeA's Rights in Data working group. The group comprises:

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

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.

This guide should be read in conjunction with the briefing note: Data Protection: A Councillor's Guide, which is a summary of this document.

# 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.

| [1.](#) Part Two deals with a few general questions raised by the Act and provides definitions of the main terms which appear in it.

| [1.](#) 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.

| [1.](#) Part Four discusses disclosure to Councillors

| [1.](#) 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
- a) Details of cases where the Councillor is acting on behalf of a constituent
- a) Personal data held for constituency purposes
- a) Lists of contacts
- a) Data held as part of the Councillor’s duties as a representative of a national body
- a) Data used for political canvassing

Formatted: Indent: Left: 0.63 cm, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at:

0. 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
0. The Councillor must also notify the Commissioner of any changes in his/her notified particulars.
0. As a Data Controller, the Councillor must comply with the data protection principles. These are set out in Appendix A.
0. 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.
0. 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.

Deleted: AHL Code of Practice2.doc

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:

- | c) An employee of the authority and therefore subject to the conditions attached to the authority's purposes and processing of personal data.
- | c) A Data Controller in his/her own right
- c) a Data Subject
- | c) 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 Councillor'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.**

Deleted: AHL Code of Practice2.doc

### *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:

**D.** 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.

**D.** Canvassing Political Support:

Included under this heading are: lists of contacts; personal information held for party political purposes;

**D.** 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 use 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](http://www.dataprotection.gov.uk).

### *The First Principle*

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

- At least one of the conditions in Schedule 2 of the Data Protection Act is met, and*
- 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?*

Deleted: AHL Code of Practice2.doc

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.

Deleted: AHL Code of Practice2.doc

**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.*

**These rights are discussed in detail at Appendix ???**

### ***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

Deleted: AHL Code of Practice2.doc

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)*

**Formatted:** Indent: Left: 0.63 cm, Hanging: 4.76 cm, Outline numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Tab after: 1.9 cm + Indent at: 1.9 cm

**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.

**Formatted:** Indent: Left: 0.63 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**Formatted:** Indent: Left: 0.63 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**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.

**Formatted:** Indent: Left: 0.63 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**Formatted:** Indent: Left: 1.11 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**Formatted:** Indent: Left: 1.11 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

**Formatted:** Indent: Left: 1.11 cm, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at: 0.63 cm

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.

**Deleted:** AHL Code of Practice2.doc

## 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

- | 8. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
  - ) At least one of the conditions in Schedule 2 of the Data Protection Act is met, and
  - ) In the case of sensitive personal data at least one of the conditions in Schedule 3 is also met. (See Appendix B)
- | 8. 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.
- | 8. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- | 8. Personal data shall be accurate and where necessary kept up to date.
- | 8. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- | 8. Personal data shall be processed in accordance with the rights of Data Subjects under this Act.
- | 8. 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,
    - a) for the exercise of any functions of either House of Parliament
    - a) for the exercise of any functions conferred on any person by or under any enactment
    - a) for the exercise of any functions of the Crown, a Minister of the Crown, or a government department, or
    - a) for the exercise of any other functions of a public nature exercised in the public interest by any person.
  1. 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.

Formatted: Indent: Left: 0.63 cm, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at:

Formatted: Indent: Left: 0.63 cm, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at:

## **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.

1. (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

1. 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.

1. 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.

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

1. 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.

1. 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.

1. 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

1. 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.

1. 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.

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

Deleted: AHL Code of Practice2.doc

## 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,
- a) is recorded with the intention that it should be processed by means of such equipment.
- a) is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system,
- a) forms part of an "accessible record" or,
- a) any recorded information held by a public authority (as defined in the Freedom of Information Act 2000)

**Formatted:** Indent: Left: 1.27 cm, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Tab after: 0.63 cm + Indent at:

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.

**Deleted:** AHL Code of Practice2.doc

*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.

|  |                |                            |
|--|----------------|----------------------------|
| <b>Page 19: [1] Deleted</b><br>AHL Code of Practice2.doc | <b>cm21104</b> | <b>16/12/2008 10:15:00</b> |
| <b>Page 19: [2] Deleted</b><br>AHL Code of Practice2.doc | <b>cm21104</b> | <b>16/12/2008 10:15:00</b> |