



|                                       |   |
|---------------------------------------|---|
| <b>POLICY TITLE</b>                   | Data Protection, Confidentiality and Access to Information Policy |
| <b>POLICY NUMBER</b>                  | GG/PO/06  |
| <b>AUTHOR</b>                         | Jeanette Bolton   |
| <b>DATE AGREED</b>                    | 14 August 2008  |
| <b>REVIEW DATE</b>                    | August 2011   |
| <b>OFFICER RESPONSIBLE FOR REVIEW</b> | Business Support Manager  |

## **DATA PROTECTION, CONFIDENTIALITY AND ACCESS TO INFORMATION POLICY**

### **1 POLICY STATEMENT**

- 1.1 Fabrick Housing Group and its partner companies need to collect and use certain types of information about people in order to operate effective and efficient business, and ensure that services appropriate to the needs of employees and customers are provided. This includes information about current, past and prospective employees, board members, suppliers, clients, customers and others with whom communications are made. For the purpose of this Policy these groups of people are referred to as data subjects.
- 1.2 Personal information must be dealt with lawfully and correctly whichever way it is collected, recorded and used; whether on paper, in a computer, or recorded on other material. There are safeguards in the Data Protection Act 1998 to ensure this.
- 1.3 The lawful and correct treatment of personal information is very important to successful organisations, and to maintaining confidence between the organisations and those with whom they deal with.
- 1.4 The Group believes that people have a right to see what information is kept about them, and fully endorses the principles of data protection, as specified in the Data Protection Act 1998 and other related legislation.
- 1.5 It aims to reach a balance between encouraging openness, avoiding unnecessary secrecy and bureaucracy and respecting an individual's and the Group's and confidentiality.
- 1.6 All information will be treated lawfully and correctly by board members, employees of the Group and its partners, and by those acting on behalf of the Group.

1.7 The members of the Group will ensure that:

- A policy is maintained for the confidentiality of information;
- Board members and employees and others acting on behalf of the Group understand the need to maintain integrity through correct operation of the policy;
- It is as open as possible in its dealings and in meeting its obligations concerning the provision of information.

## 2 REFERENCE MATERIALS

2.1 Related documents supporting the Policy are:

- Data Protection Act 1998: Definitions (Appendix 1);
- Data Protection Principles (Appendix 2);
- Data Protection Act 1998: Good Practice Guide (Appendix 3);
- Guidance notes from the Information commissioners Website.

## 3 DEFINITIONS

3.1 For the purposes of this Policy all definitions are shown within Appendix 1 attached.

**The Group** – Fabrick Housing Group, The Group Limited, Tees Valley Housing Limited and any other Subsidiary Companies.

## 4 POLICY CONTENT

4.1 Obligations

4.1.1 In compliance with the Act, the Group will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information in a confidential manner ensuring that the data held is not excessive but sufficient to fulfill operational needs or to comply with any legal requirements;
- Will dispose of data when it is no longer required (subject to any statutory requirements);
- Ensure that necessary and sufficient steps are taken to ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act. These include:
  - a) The right to be informed that processing is being undertaken;
  - b) The right of access to one's personal information;
  - c) The right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.

- Take appropriate technical and organisational security measures to protect personal information against damage, loss, misuse or inappropriate disclosure;
- Ensure that transfer of data is done in a lawful manner with due regard for security;
- Ensure that personal information is not transferred abroad without suitable safeguards and appropriate contact for use is in place.

4.1.2 In addition, The Group will also ensure that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good Data Protection practice;
- Everyone managing and handling personal information is appropriately trained to do so and is appropriately supervised;
- Anybody wanting to make enquiries about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with and methods of handling personal information are clearly described;
- All activities relating to the processing of personal data have sufficient safeguards and controls in place for security of data including a request for identification where required;
- All contracts with third parties that involve processing of personal data will make reference to the obligations and necessity of compliance with the Act;
- A regular review and audit is made of the way personal information is managed and that methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- There is someone with specific responsibility for Data Protection and related legislation in the organisation.

## 4.2 Handling Confidential Information Inside and Outside of the Workplace

4.2.1 Whilst carrying out work for The Group employees and board members will come into contact with sensitive information that is personal or not ready for distribution. To ensure that this information remains confidential employees and board members will:

- Use personal passwords provided for computer access and not share these passwords with others;
- Ensure that conversations relating to personal or confidential matters are held in an appropriate location, where enquiries are being made in a reception area private interview facilities will be made available should these be requested, and officers will take into account who may be listening, when holding a conversation.
- Will clear personal or confidential information from desks and retain it in locked cabinets at the end of the working day.
- Ensure that confidential information to be posted, internally or externally is clearly marked as such.

- If employees or board members take documents or information away from the office (hardcopy or electronically) they will take appropriate action to ensure that the information remains secure by storing items safely out of view, for example items will not be left in vehicles when parking or laptops left unattended.
- Ensure that if documents or laptops are being worked on when using public transport that every care is taken to ensure that the documents/laptop is not being overlooked and that they take the items with them when leaving the transport.
- Ensure that any confidential items to be discussed in meetings are on grey paper and included at the end of an agenda. All who are not required for the decision making process on the matter will be asked to leave the meeting.

### 4.3 Data Protection Requirements

4.3.1 The Data Protection Act 1998 requires that eight principles are followed when handling personal data. These are shown in detail in Appendix 2 of this Policy, however, in short they say that information:

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purpose(s), and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Shall be accurate and, where necessary, kept up-to-date;
- Shall not be kept for longer than is necessary for that purpose or purposes;
- Shall be processed in accordance with the rights of data subjects under this Act;
- Shall be secure and that 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;
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

4.3.2 Any person may exercise the right to request personal data held about them by submitting a written request (as guided by the Act) to the Group's designated Data Protection Officer. Along with the request, The Group will request a payment of £10.

4.3.3 Once received and payment is made, the data subject will receive a response within 40 calendar days. If there is insufficient information provided with the request to assist in identifying and locating data The Group is not obliged to provide the information.

#### 4.4 Security of types of data held

##### 4.4.1 Paper records

Sensitive information such as rent arrears, medical details, ethnic origin, domestic violence, etc will be kept secure at all times, and access to files will be restricted to identified officers of The Group. This will be achieved through a combination of restricted access to offices and locked file storage systems.

##### 4.4.2 Computerised records

Sensitive information will be held secure within the IT systems, and access to data will only be given to those who need it for the performance of their duties. All systems will be password protected to minimise the risk of information being accessed by unauthorised users. Officers are advised that passwords are not to be disclosed to others, and using other officers' access permissions is a serious disciplinary offence.

##### 4.4.3 Housing Applications

Applications for re-housing will be dealt with by the partner companies within The Group therefore applicants:

- Will be provided with a password in order to use the Choice Based Lettings system;
- May have access to information held about themselves and their family held for the purpose of the application; however information relating to the applicant and a third party is only available with the written agreement of the other person;
- Will not be given access to information that identifies a third party or information that has been given by a third party unless the third party agrees to it being seen;
- Cannot have access to information where there are legal reasons for the information not being released;
- Have the right to request in writing for the removal or correction of any information recorded about them which they believe to be inaccurate. If the Group agrees that this is the case, the record will be corrected and the applicant will be able to see the correction. If the Group **does** not agree that the information is inaccurate, an explanation as to why this is the case will be provided and a note made of the applicant's view on the applicant's records.

Deleted: do

##### 4.4.4 Third party requests for information

The Group is happy to pass on any correspondence on behalf of third parties who wish to contact a tenant or former tenant but under no circumstances will the address be divulged.

##### 4.4.5 Press Enquiries

All press enquiries will be referred to the Communications and Media Officer who will act as the liaison officer.

#### 4.4.6 Board Members' Requests

Board members have no rights to be given any personal information about anybody, unless the information is required for a specific confidential report to be presented to the Board.

#### 4.4.7 Councillor, MP and Mayoral Requests

Councillors, MPs and the Mayors have no rights of access to personal information unless the person whom the information relates to has provided confirmation that information may be shared.

#### 4.4.8 Contracts and other Records

All contracts will contain a confidentiality clause preventing:

- Disclosure of any of The Group's records by any contractor to a third party without prior written agreement from the Group;
- Disclosure by The Group to any third party of any tender information provided by the contractors submitting the tender.

4.4.9 Board members and employees must keep secure all records of a confidential nature. The disclosure of information to third parties as part of a collaborative process, which enables a contractor to submit a successful bid, will be seen as a serious breach of this policy and the Code of Conduct in place for board members and employees. Any disclosure may result in disciplinary offence for employees.

4.4.10 In certain circumstances, information is not made available, and will be kept confidential. Such circumstances may include:

- Where a individual wishes the information to remain confidential;
- Sensitive personal data, for example information relating to illness, race or ethnic origin;
- Sensitive organisational data which could damage or threaten the security of The Group;
- Commercially sensitive data, which could be used to secure financial or competitive advantages over the Group.

#### 4.5 Disclosure of information to other parties

4.5.1 In some exceptional circumstances, it may be appropriate to divulge a request for information to specific third parties, for example, to prevent a criminal offence from being committed, or to prevent the continuation of a criminal offence. In many such cases, the disclosure could be forced through a legal application for subpoena. In such circumstances, the information may be disclosed at the discretion of the Group, such disclosures should be agreed by the Group Company Secretary prior to the disclosure. Exceptional circumstances can include:

- Co-operation with the police, where there is reasonable evidence of a crime being committed by an individual, or where the information is to be provided under the provisions of the Crime and Disorder Act 1998;
- Co-operation with Housing Benefit providers where requests are received in writing and there is reasonable evidence of a benefit fraud being committed;

- Discussing individuals' circumstances with the Housing Benefit or the Benefits Agency or with agencies such as the Citizens Advice Bureau. In most cases, a signed form authorising the disclosure will be requested and this will be held on file in these circumstances;
- Sharing information when using a tracing agent for the collection of former tenants' arrears and other debts owed to the Group, passed to them as part of the debt recovery process;
- Giving information to third parties where a protocol has been drawn up and agreed between the parties and agreed by the Board and where the protocol forms part of the proper operation of activities.

4.5.2 It is difficult to cover all eventualities where a disclosure may be necessary and any disclosure outside this Policy may therefore be authorised by the Group, Company Secretary, or the appropriate Managing Director.

#### 4.6 Data Security Breach

4.6.1 A data security breach can happen for a number of reasons, for example:

- loss or theft of information on which data is stored
- Unauthorised access;
- Equipment failure;
- Human error;
- Unforeseen circumstances e.g. fire/flood.

Deleted: Unforeseen

Deleted: circumstances,

4.6.2 If a breach occurs it is important that:

- The breach is contained and if possible the information recovered;
- An assessment of ongoing risk is made;
- There is notification of the breach;
- There is evaluation of the effects of the breach and the response.

4.6.3 If a breach does occur, either accidentally or deliberately, as soon as this is recognised the Group will take immediate action. If deliberate action was taken to disclose information serious disciplinary action may be taken, which could lead to dismissal of an employee or board member.

4.6.4 The Group Company Secretary will be informed of any accidental or deliberate disclosures that do not meet with the requirements of data protection and this Policy, and in conjunction with the service director, Managing Director or Group Chief Executive will decide an appropriate course of action. This will take into account:

- The type of data involved and how sensitive it is;
- Review of protections in place if data is lost or stolen, what the data could tell a third party about someone and whether this information could be used in a harmful way;
- Whether those affected by the release or loss of the information needs to be informed.

4.6.5 Further guidance on data security breaches is available from [www.ico.gov.uk](http://www.ico.gov.uk)

## 5 EQUALITY AND DIVERSITY

- 5.1 The Group recognises that it operates in a community within which there is wide social diversity, and is committed to providing equal opportunities and valuing diversity.
- 5.2 Where required, assistance will be given to people who wish to make a request for information using this policy but have difficulty in doing so because of circumstances such as disability or language comprehension.

## 6 CUSTOMER INVOLVEMENT

- 6.1 As legislation and good practice dictates the contents of this Policy there is no requirement for customer consultation.

## 7 MONITORING AND REVIEW

### 7.1 Monitoring

- 7.1.1 The Group Director of Corporate Services has responsibility, along with the designated Data Protection Officer on behalf of the Group Chief Executive, for ensuring that this Policy is implemented.
- 7.1.2 Requests for information will be recorded and reported as required.
- 7.1.3 Complaints concerning breaches of the Data Protection provisions or other failure to comply with the Policy will be dealt with through the Complaints Procedure.

### 7.2 Review

- 7.1.1 The Policy will be reviewed every three years or sooner if legislation requires it.

## 8 RESPONSIBILITY

- 8.1 The Group Director of Corporate Services on behalf of the Group Chief Executive and Managing Directors ~~are~~ responsible for the implementation of this Policy.

Deleted: is

## Data Protection Act 1998: Definitions

### 1 INTRODUCTION

- 1.1 This appendix outlines in more detail the definitions of terms used within the Data Protection Act 1998: Good Practice Guidance, which offers advice on how the Act should be applied to the practical everyday activities.
- 1.2 Under the Act the Information Commissioner has powers to issue an enforcement notice or an information notice where a Data Controller has contravened any of the Data Protection principles. The main contraventions are likely to be unauthorised processing and/or disclosure of data. Failure to comply with such a notice is an offence under the Act.
- 1.3 It is therefore vital that individual members of employees acquaint themselves with the requirements of the Act and ensure that they comply with it. If necessary, The Group will rely on a defence of due diligence, based on the information about the Act which is made available to employees.

### 2 DEFINITIONS OF TERMS USED WITHIN THE DATA PROTECTION ACT 1998

- 2.1 **Data-Information** which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or (b) is recorded as part of a relevant filing system.
- 2.2 **Personal Data** – Data that relates to a living individual, which can be identified from the data, includes any expression of opinion about the individual and any indication of the intentions of the data controller in respect of the individual. Note that this includes photographs, e-mail messages and data recorded by CCTV. It also covers data identified by reference numbers where a separate list can be used to match the reference numbers to named individuals.
- 2.3 **Sensitive Personal Data** – Personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs, (d) whether they are a member of a Trade Union, (e) their physical or mental health, (f) their sexual life, (g) the commission or alleged commission by them of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by them.
- 2.4 **Data Controller** – The person or organisation responsible for the manner in which any personal data is processed. Note that The Group is the Data Controller; individual members of employees process data on behalf of The Group are referred to as Data Users, an internal term which does not appear in the Act as such.
- 2.5 **Data Processor** – Any person who processes the data on behalf of the Data Controller.
- 2.6 **Data Subject** – An individual who is the subject of personal data.

- 2.7 **Processing** – Obtaining, recording or holding the data or carrying out any operation on the data, including organising, adapting or alteration of the data; retrieval, consultation or use of the data. If in doubt, assume that it is processing.
- 2.8 **Relevant filing system** – Any set of information relating to individuals relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically, the set 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. Note that this definition extends the Act to include manual files which contain information about an individual, such as personal files.

## 1 Data Protection Principles

- 1.1 There are Eight Principles specified in the Act with which a Data Controller must comply. The Eight Data Protection Principles are based on three key concepts:
- Purpose – personal data must only be held for a clear purpose or purposes;
  - Fairness – personal data must only be processed for legitimate purposes;
  - Transparency – data subjects must be given certain basic information about the personal data held about them.

## 2 First Principle – fair and lawful processing

- 2.1 “Personal data shall be processed fairly and lawfully and shall not be processed unless certain conditions are met”.
- 2.2 This Principle aims to ensure that individuals are made aware of how their personal data will be used and covers both the original obtaining of data, for both computer and manual files, and its subsequent processing. To ensure fairness, certain information must be given to the data subject at the point of collection. This comprises:
- The identity of the data controller, i.e. The Group;
  - A note of the purposes, in fairly general terms, for which the data is being collected, and;
  - Any other information thought necessary.
- 2.3 The Group meets this requirement as far as its employees and customer records are concerned by the use of standard wording on appropriate forms. Where services subsequently make use of data, which was originally collected centrally, there is no need for them to provide additional information to the data subjects, provided that they will be using data within the original purposes. If they wish to use the data for new purposes, this must be notified to the data subjects concerned by the department.

## 3 Second Principle – purposes for holding data

- 3.1 “Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes”.
- 3.2 This Principle covers the identification of the purposes for which data is processed and the restriction of processing to those purposes. The Group makes use of fairly general definitions of purpose in collecting data centrally, for example, the provision of accommodation or for employment purposes. It is important to note however that such data can only be processed for those explicit purposes. In other words, data collected for accommodation purposes cannot be subsequently used for financial purposes unless both purposes were identified at the time of original collection of the data.

If data is required to be processed for any purpose other than the original one, the data subject must be notified before processing can take place. The Data Protection Officer will be happy to advise if the situation arises.

#### **4 Third Principle – status of data**

- 4.1 “Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed”.
- 4.2 This Principle requires that all data held must be justified in relation to the stated purpose for which it is held. In collecting data therefore it is important to ask whether the data is really needed for the purposes concerned. If the answer is “no”, the data must not be collected. It is equally important to review the amount of data being collected from time to time to ensure that it is still relevant.

#### **5 Fourth Principle – accuracy of data**

- 5.1 “Personal data shall be accurate and, where necessary, kept up-to-date”.
- 5.2 This Principle requires that the data held is always accurate and, except in the case of historic data kept for archive purposes, up-to-date.
- 5.3 In holding data, therefore, procedures must be put in place (i) to ensure that data is accurate and (ii) to enable data to be updated. This is particularly important in the case of, for example, contact data, where data subjects must be made aware of the procedures to notify changes of address, etc. It is accepted that data subjects will not always avail themselves of these procedures, and that data may be inaccurate through no fault of the data user, but as long as procedures are in place and have been notified to the data subject, there is no need to take further action.

Deleted: subject ,

#### **6 Fifth Principle – retention and disposal of data**

- 6.1 “Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes”.
- 6.2 This Principle covers the retention of data for the purpose concerned and its subsequent disposal. No data must be kept for longer than is necessary to carry out the purpose concerned. The length of time will vary greatly with the type of data being held; in some cases it might be appropriate to retain it for only a very short time, in other cases it might be necessary to retain it indefinitely, some retention periods are even governed by statute.
- 6.3 Once a retention policy is in place, appropriate procedures to dispose of the data must also be put in place. Security is very important in the disposal of personal data.
- 6.4 If data is to be retained for archive purposes, the Third Principle must be taken into account.

## **7 Sixth Principle – rights of data subjects**

7.1 Personal data shall be processed in accordance with the rights of data subjects under the Act.

7.2 This Principle covers a number of rights, which data subjects have with respect to their own data. These are (i) rights of subject access, (ii) rights to prevent processing, including direct marketing, (iii) rights of compensation for substantial damage or distress, (iv) rights to have data amended or deleted, and (v) rights relating to automated decision-taking.

- Subject access: Data subjects have the right to have access to their personal data. This is probably the most important of the data subject rights. It is also the right of which most data subjects are aware. See Data Protection Good Practice Guidance at Appendix 3 for details of how subject access requests are handled by The Group;
- Prevention of processing including direct marketing: The Act includes an important right to prevent processing, in particular direct marketing. This relates to any information sent out to a data subject that is not directly concerned with The Group business. For example, flyers sent to customers about unrelated products for sale by a third party. Anyone likely to engage in direct marketing must have procedures in place to enable a data subject to object being the target of direct marketing and to have their name removed from any such lists;
- Compensation for substantial damage or distress: Data subjects are entitled to claim compensation for any substantial damage or distress caused to them by improper use of their personal data. For example, if the data held is found to be inaccurate or excessive, possibly following a subject access request, the data subject can sue The Group for compensation if they can prove that substantial damage or distress has been caused. This is especially important with respect to sensitive data, which is most likely to cause damage or distress to a data subject;
- Amendment/deletion of data: Data subjects are entitled to request the amendment or deletion of inaccurate or irrelevant data. Such requests are most likely to follow subject access requests.
- Automated decision-taking: Data subjects have the right to be informed if any decisions that are taken about them solely by means of automated decision-taking procedures and to request that such procedures be stopped. Where decisions are taken entirely by automated means, data subjects must be informed of this and the practice must cease if a data subject objects.

## **8 Seventh Principle – disclosure of data**

8.1 “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”.

- 8.2 This Principle covers both the disclosure of data and the unauthorised or unlawful processing of data. It is probably the single most important Principle and the easiest to get wrong. The Data Protection Good Practice Guidance shown in Appendix 3 provides advice relating to a number of The Group specific scenarios to ensure maximum understanding of the disclosure issue and to highlight its importance.
- 8.3 Data security is another way of looking at disclosure and is equally important as far as the Seventh Principle is concerned. Various measures must be taken to ensure that data is kept secure:
- Technical measures: network security; the proper use of passwords;
  - Organisational measures: the physical security of computers and files in cabinets, locked rooms, ensuring that computer screens cannot be overlooked;
  - Accidental loss, destruction or damage to data has the same effect as an unauthorised disclosure. Good back-up procedures must be in place and used effectively. These should include procedures to recover lost data.
- 8.4 It is particularly important to be aware of data security when processing data off-site, especially when using a laptop in a public place such as a train.
- 8.5 Data Processor is the technical term for anyone who processes data on behalf of a Data Controller; the term used to be "Computer Bureau". The Group will ensure that any third parties who have access to confidential information regarding tenants or employees meet with the Data Protection Act by:
- Including in any SLA an explicit clause that refers to the Data Protection Act 1998;
  - The Processor agrees to adhere to the Eight Data Protection Principles; and
  - The Processor operates at the same level of data security as The Group.

## **9 Eighth Principle – transfer of data**

- 9.1 "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".
- 9.2 A requirement of the Act is that data must not be transferred to any country that lies outside the European Economic Area (EEA). The EEA comprises the countries of the EU together with Norway, Iceland and Liechtenstein.
- 9.3 This means that data cannot be transferred electronically to the greater part of the world unless similar and adequate data protection legislation is in place there. There concern is with the level of data security in the country concerned and transfer can take place if, following an individual assessment of the circumstances, it is felt that the data will receive the same level of protection and security as in the UK.

## Data Protection Act 1998: Good Practice Guidance

### 1 Introduction

- 1.1 The following guidance provides simple and accessible advice to employees and board members involved in the handling of personal data and is designed to develop better understanding of The Group's obligations under the Data Protection Act 1998 ("The Act"). It provides solutions to the kinds of every day problems encountered by employees who handle personal data, particularly in relation to disclosure of data, and urges regular contact with the Data Protection Officer who is responsible for compliance with the Act. Please note that "data" has been referred to throughout as a single noun.
- 1.2 The guidance is intended to provide advice only and does not suggest that all employees and board members would be involved in all the scenarios listed. It is still important that the relevant service handles specific tasks and requests, in the usual way.
- 1.3 The guidance is a 'live' document that will continually be updated to cover new issues as they arise. If you wish to seek advice on a particular issue or problem that is not covered, please contact the Data Protection Officer.

### 2 Data Protection Act: The Facts

- 2.1 A Broad View of the Act
  - 2.1.1 The Act provides various safeguards relating to the management of individuals' personal data. Naturally, it places a number of obligations on The Group to ensure data is managed effectively and lawfully.
  - 2.1.2 The Act defines "personal data" as any data that relates to a living individual who can be identified from it. This includes personal images and audio recordings as well as text.
  - 2.1.3 It is also important to note the term "processing", which is a generic term used in the legislation to describe any action taken in relation to personal data, such as for example obtaining, recording, holding, adapting, retrieving, altering, disclosing or destroying. If you are in any doubt when handling personal data always assume you are "processing" it.
  - 2.1.4 The 1998 Act updated the previous 1984 Act, which had come about as a result of concern over the management of personal data held in computerised records. Significantly, the 1998 Act brought 'structured' manual data within the scope of its provisions. The Freedom of Information Act 2000 then amended the Act to cover manual data held in an 'unstructured' form. Consequently, the Act does not now differentiate between any kind of electronically or manually held data.

## 2.2 Data Protection Principles

- 2.2.1 The Act is based on a number of principles as detailed in Appendix 2 of the Data Protection, Confidentiality and Access to Information policy, which act as an excellent guide towards ensuring compliance.

## 3 How Subject Access Right Requests are handled

- 3.1 Any person may exercise the right to request personal data held about them by submitting a written request to the Data Protection Officer. Where required, assistance will be given to people who wish to make a request for information using this policy but have difficulty in doing so because of circumstances such as disability or language comprehension.
- 3.2 In line with the Act, The Group will only accept written requests from individual who wish to access their data. If an individual approaches you requesting such access, they should be issued with the "Data Subject Access Application Form" which details what they are required to do. It is policy to make a charge of £10 for each official subject access request.
- 3.3 This form should be completed by the data subject, signed, dated and returned together with the fee and proof of identity as required to the Data Protection Officer. The form acts as a record of the request, but also enables the individual's records to be identified more easily and provides a declaration from the individual that they are who they say they are.
- 3.4 Once the Data Protection Officer has received the form and cleared payment, the request must be processed within forty calendar days. This deadline period does not commence and The Group is not obliged to release any information until the form has been received and payment has cleared. Equally, The Group is not obliged to provide any data unless sufficient information is provided to identify the data subject and locate any data, which it might hold.

## 4 Processing General Personal Data

- 4.1 Personal data is being processed throughout The Group all the time by a significant proportion of employees and board members.
- 4.2 At the beginning of an individual's relationship with The Group, they are notified of the need and intention to process their personal data and are also informed of the purposes for that processing. Consent is also obtained where necessary for data to be held, either through their tenancy agreement or in the case of employee, through the employee handbook.
- 4.3 Once the Data Protection Officer has received the form and cleared payment, the request must be processed within forty calendar days. This deadline period does not commence and The Group is not obliged to release any information until the form has been received and payment has cleared. Equally, The Group is not obliged to provide any data unless sufficient information is provided to identify the data subject and locate any data, which it might hold.

4.4 Consent is normally the best (and most common) route to enable data of this kind to be processed. When in doubt, if you have the individual's consent, you are covered as far as data protection legislation is concerned. It should be noted though that the Act does allow other ways to process data without obtaining consent. These are:

- For the performance of a contract;
- For compliance with any legal obligation to which The Group is subject, other than an obligation imposed by contract;
- To protect the vital interest of the data subject;
- For the administration of justice;
- To exercise any functions brought about by other legislation;
- To exercise any functions of the Crown, a Minister of the Crown or a Government Department;
- To exercise any functions of a public nature exercised in the public interest by any person, and;
- For the purposes of legitimate interests pursued by The Group or by a third party requesting data (except where the processing may prejudice the rights and freedoms or legitimate interests of the data subject).

## **5 Processing sensitive personal data**

5.1 The Act provides a separate definition for "sensitive personal data". This relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, Trade Union activities, physical or mental health, sexual life, or details of criminal offences.

5.2 As with general personal information, there are a number of circumstances that enable the processing of sensitive personal data without consent. However, if consent is used as a way to process such data, it is important to note that the Act requires explicit consent. In cases where individuals have submitted sensitive data about themselves, this can be considered as consent in itself for the data to be processed, although it is still important to keep the individual informed about how the data is being used.

5.3 Circumstances that enable sensitive data to be processed lawfully, other than explicit consent are:

- The Group's activity relating to employment;
- To protect the vital interests of an individual where consent cannot be given (such as medical emergency);
- Where The Group cannot reasonably be expected to obtain consent;
- To protect the vital interests of an individual where consent has been unreasonably withheld;
- Legitimate activities carried out by The Group;
- Where the data has already been made public by the data subject;
- For legal proceedings (including prospective legal proceedings);
- To exercise any functions brought about by other legislation;
- To exercise any functions of a public nature exercised in the public interest by any person;

- For medical purposes undertaken by a health professional, or equivalent, and;
- For equal opportunity purposes.

5.4 Sensitive information must be protected with a higher level of security. It is recommended that sensitive records be kept in a lockable cupboard, drawer or filing cabinet or in a password-protected computer file.

## 6 The Subject Access Rights

6.1 The Act provides the “subject access right” which enables individuals, subject to certain specific exemptions, to receive an intelligible copy of all personal data held about them by The Group. The right extends to all data whether held manually or electronically.

6.2 By allowing such access to data the “subject access right” has significant implications for The Group. It is important to note that personal data contained within e-mails is subject to access requests.

6.3 If an individual requests to see data relating to them which then turns out to be for example inaccurate, out of date, held unnecessarily or offensive, The Group may be liable for prosecution.

## 7 Third party data and the subject access rights

7.1 Potentially, when an individual makes a “subject access request” shown as Appendix 4 it may not be possible to provide some of the data without disclosing information relating to another individual. Under these circumstances, The Group is not obliged to provide the data in question unless the other individual has consented to its disclosure or it is reasonable to do so without the consent of the other individual. In determining whether it would be reasonable, The Group must consider any duty of confidentiality owed to the other individual; any steps taken by The Group to seek consent; whether the other individual is capable of giving consent; or any express refusal of consent by the other individual.

7.2 It is important to note the implication of third party data when supplying information for a “subject access request”, and raise any doubts with the Data Protection Officer.

Deleted: supplying information

## 8 Practical Tips: Applying Data Protection requirements to The Group Activities

8.1 Data Sharing within The Group

8.1.1 In data protection terms, The Group is considered to be the data controller; a single entity processing personal data about a large number of individuals. This means that “disclosure of data” is considered to have taken place if it has passed outside The Group to an external third party. This does not mean however that data can be shared freely within the Group. The first data protection principle states that data must be processed fairly. It would be grossly unfair if personal data were passed unnecessarily between Group employees without good reason. Consequently, if somebody asks you for access to an individual's personal data, it

is vital to ascertain the purpose of the request. Disclosure must only then be made if you are satisfied that the other person needs it to do their job. If this is not the case or it is unclear, contact the Data Protection Officer who will help to confirm whether disclosure is possible.

## 8.2 Displaying photographs

8.2.1 In some services and sections of the Group, it is common practice to post photographs of employees on notice boards and web pages, along with some biographical information. While this is not illegal under the Act it is worth noting that an individual is entitled to refuse to have their photograph or personal information published in this way even if access is limited to the Group's internal publishing. It is good practice (and ensure The Group is operating in the spirit of the Act) to check with the individuals concerned before proceeding.

## 8.3 Remote and home working

8.3.1 When working from home or remotely, the same level of adherence to the data protection principles must be maintained in relation to personal data. Special care should be taken in the transport of personal information.

## 8.4 Implications of e-mail

8.4.1 When writing and dealing with e-mails always have regard for the principles of the data protection legislation and think about how they affect what you are doing. Writing or processing an e-mail should always be viewed in the same light as a letter or a fax. A simple test is to establish whether you would be happy including the information in a letter. If not, do not include it in an e-mail. If not, delete it immediately.

8.4.2 Equally, you should always consider the implications of distribution lists if sending an e-mail that includes personal data. For example, sending somebody's address or contact details to the 'all employees' distribution list is unacceptable under the terms of the Act. Even if the motive is well meaning, it is considered to be unfair processing of the individual's data and action could be taken against The Group. There is also the potential for unwarranted disclosure of data outside The Group if distribution lists are used in this way. For further information, please refer to Managing electronic Mail: Good Practice Guide.

## 8.5 Maintaining Files of Individuals

8.5.1 For files held on both employees and customers, it is common practice to file and maintain all relevant data relating to an individual as a record of that person's time working or as a tenant. While this makes sense for most of the time, sometimes it can be very dangerous as all information contained within these files falls within the scope of the Act. Therefore, those responsible for maintaining individual employees or customer files must always consider adherence to the data protection principles. Data subject access rights enable individuals to obtain copies of their files on request, and thus see what information is held about them. It is vital that offensive, derogatory or damaging remarks are **never** kept on file. This applies equally to e-mails that are printed, notes of meetings or conversations, or any other way in which data of this kind could be processed.

- 8.5.2 When deciding if something should be filed, you must always ask yourself if you would feel happy with the individual in question seeing what had been written about them. If not, do not include it on the file. It is often more sensible to have verbal conversations about individuals if the issues in question are sensitive.
- 8.6 Publishing Names and Personal Data on the Group websites
- 8.6.1 Publishing personal data on the internet discloses it automatically on a worldwide basis. If not done in the correct way, you leave The Group open to charges that it has contravened the Act by failing to hold data securely or prevent it from reaching countries outside the European Economic Area that do not have in place similar data protection measures. The simple answer to this is to refrain from publishing personal data in this way unless it relates to an individual's official role or function in relation to The Group. For example, providing the name and contact details of a specific officer of The Group, or that they serve on a particular committee, is legitimate and is an essential part of the purpose of the websites, whereas providing somebody's home address or telephone number (or indeed more personal information) is not.
- 8.6.2 In order to comply with the 'fair processing' elements of the Act, it is also important that anybody whose name and/or data appears on the websites is aware that it is there and that mechanisms are in place to enable them to object and if necessary to have it removed. This applies to data available on both The Group intranets and through the worldwide web, as well as to employees and customers alike or any other individual whose details may appear.
- 8.6.3 Please note that if an individual has given explicit consent for any of their personal data to be published in this way, it is permissible to do so.
- 8.7 Internal Request for Personal Information
- 8.7.1 Often when requests for personal information about a third party individual are made internally from one part of The Group to another, employees are told that the information cannot be disclosed because of data protection. This is not true. If you need the information to do your job, you have a right to see it. We tell employees that their personal data is "only disclosed to employees within The Group who need to know it in order to carry out their duties". The Group is a single data controller so we are not technically disclosing data unless it goes outside the organisation. While it is not good practice to pass data around in ways, which could lead to inadvertent disclosure, targeted disclosure made on a need-to-know basis is perfectly legal under the DPA and is the desirable way to proceed.

## **9 Practicle Tips: Third party requests for personal data**

### 9.1 Requests from Police or other official bodies

9.1.1 Occasionally, The Group receives requests from the police and officials for personal information. Disclosing data under these circumstances is not compulsory unless The Group is served with a Court Order. However, The Group will always aim to assist any officials as far as possible and particularly as the Act does allow disclosure of data if it relates to:

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

9.1.2 Consequently, disclosure can be made in limited circumstances. In these cases, before proceeding, employees should confirm with the police that the reason for the request is that they wish to contact a named individual about a named criminal investigation (regardless of whether that individual is a suspect or witness) and that failure to release the data would prejudice the investigation. Good practice is to request written confirmation of this by a senior officer. Most police forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29 of the Data Protection Act, a brief outline of the nature of the investigation and the subject's role in that investigation, and the signature of the investigating officer. If there is ever any doubt, please contact the Data Protection Officer.

### 9.2 Requests from Immigration Officials

9.2.1 The Group may receive requests from immigration officials. Section 35 of the Data Protection Act allows us to disclose information if it is required by law to do so. An immigration official making a genuine enquiry about an individual would know about and be happy to disclose details of any such legal requirement on their part. Equally, the Data Protection Act allows disclosure of personal data "for purposes of legitimate interests" pursued by The Group and any immigration official. Although a case-by-case analysis must always be made, it is likely that immigration enquiries would also fall into this category. As with all external requests for personal information, verifying the identity of the person requesting the data and the purpose of the request is important. If there are time pressures, the minimum security option is to take a number and call the enquirer back. It is generally recommended that all enquirers should be asked to submit their request in writing on headed paper.

### 9.3 Employees e-mail addresses and contact details

- 9.3.1 Occasionally, employees receive requests from individuals for employees contact details to enable distribution of information relating to a social, professional or housing-linked event. Allowing access to contact details for this purpose is permissible under the Act, as long as it is done in a limited way. To cover this eventuality, employees are made aware that their data could be processed for this purpose. Employees should never pass personal data on to profit-making organisations or individuals. Any doubt should be discussed with the Data Protection Officer.

## Data Subject Access Application Form

Under the terms of the Data Protection Act 1998, an individual is entitled to ask for a copy of all the personal information which is held about him/her for the purposes of providing services to the individual. The information which is held about him/her for the purposes of providing services to the individual. The information, which you are entitled to receive includes a description of the purposes of the information, details of who the data is disclosed to and the sources of the data. The entitlement is known as the "Right of Access to Personal Data". A charge of £10 is made for provision of this information.

If you would like access to the personal data held about you please complete the details required on this form and return it to Data Protection Officer, 4<sup>th</sup> Floor, Centre North East, 73-75 Albert Road, Middlesbrough TS1 2RU, along with the required payment (payment should be by cheque or postal order, made payable to Erimus Housing if the request is to Tees Valley Housing). Alternatively you may take the form and payment to a housing office who will forward the request to the Data Protection Officer.

|                         |  |
|-------------------------|--|
| <b>Personal Details</b> |  |
| Name: .....             |  |
| Present Address: .....  |  |
| Post Code: .....        |  |
|                         |  |
|                         |  |
|                         |  |
|                         |  |

**Data Subject Access Application Form**

Under the terms of the Data Protection Act 1998, an individual is entitled to ask for a copy of all the personal information which is held about him/her for the purposes of providing services to the individual. The information, which you are entitled to receive includes a description of the purposes of the information, details of who the data is disclosed to and the sources of the data. This entitlement is known as the "Right of Access to Personal Data". A charge of £10 is made for provision of this information.

If you would like to access the personal data held about you please complete the details required on this form and return it to Data Protection Officer, 4<sup>th</sup> Floor, Centre North East, 73-75 Albert Road, Middlesbrough TS1 2RU along with the required payment (payment should be by cheque or postal order made payable to xxxxxxxxxxxx). Alternatively you may take the form and payment to the local housing office who will forward the request to the Data Protection Officer.

|  |                     |
|--|---------------------|
| <b>Personal Details</b>  |                     |
| Name: .....  |                     |
| Present Address .....  |                     |
| Post Code: .....   |                     |
| Telephone No.<br>Home .....  | Date of Birth ..... |
| Mobile .....   |                     |
| Length of time at this address .....Years .....Months  |                     |
| If you have lived at this address for less than two years, please supply your previous address<br>.....<br>..... |                     |
| Postcode .....   |                     |
| Length of time at this address .....Years.....Months   |                     |

**2 Data Processing**

Erimus Housing/Tees, Valley Housing Ltd/Fabrick Housing Group use personal data for the purposes shown below if you would like to access personal data held about you for all of these please tick the box marked all. If you have only used some of these please tick the box opposite the purpose(s) you wish to access.

Deleted: Fabrick Housing Group/Tees  
Deleted: The G  
Deleted: Ltd

|                         |  |  |                   |  |
|-------------------------|--|--|-------------------|--|
| All services            |  |  | Rehousing         |  |
| Rents                   |  |  | Repairs           |  |
| Regeneration programmes |  |  | Estate Management |  |
| Complaints              |  |  |                   |  |

**3 Data Subject Declaration**

In exercising the right granted to me under the terms of the Data Protection Act 1998, I request that you provide me with a copy of the personal data about me which you proceed for the purposes I have indicated in section 2 of this form.

I confirm that the above is all of the personal data I am requesting access to which is held. I also confirm that I am the data subject (the person that the data is held about) and not someone acting on his/her behalf.

Signed: Mr/Mrs/Ms/Title  
Date: .....

**4 This section is to be completed by any person(s) acting on behalf of the data subject (the person that the data is held about).**

Deleted:

Name: .....

Address: .....

Postcode .....

Telephone No: .....

I confirm that I am acting on behalf of the data subject and attach proof of my authority to do so

Signed: .....

Date: .....

**Fabrick Housing Group/Tees Valley Housing and The Group is committed to equality and diversity. We require this information to ensure that our services are delivered fairly and equally to everyone. This information you give is strictly confidential and we will use it for statistical and monitoring purposes only.**

**Equal Opportunities Monitoring Information**

**Gender** Male  Female

**Age** (please tick appropriate box)  
 16-24  25-29  30-39  40-49  50-59  60 and over

**Disability**  
 Do you consider yourself to have a disability? Yes  No

**Origin of Person making request**

|                               |  |  |  |
|-------------------------------|--|--|--|
| White                         | British <input type="checkbox"/>                 | Irish <input type="checkbox"/>         | Any other White background (please state) <input type="checkbox"/> |
| Mixed                         | White & Black Caribbean <input type="checkbox"/> | White & Asian <input type="checkbox"/> | White & Black African <input type="checkbox"/>                     |
|                               |  |  | Any other Mixed background (please state) <input type="checkbox"/> |
| Asian or Asian British        | Indian <input type="checkbox"/>                  | Bangladeshi <input type="checkbox"/>   | Pakistani <input type="checkbox"/>                                 |
|                               |  |  | Any other Asian background (please state) <input type="checkbox"/> |
| Black or Black British        | Caribbean <input type="checkbox"/>               |  | African <input type="checkbox"/>                                   |
|                               |  |  | Any other Black background (please state) <input type="checkbox"/> |
| Chinese or other ethnic group | Chinese <input type="checkbox"/>                 | Bangladeshi <input type="checkbox"/>   | Any other Asian background (please state) <input type="checkbox"/> |

Religion/Faith: How would you describe your religion/faith?  
 My religion/faith is .....

I am not religious  I prefer not to say