POLICY

General Data Protection Regulations

Wellhouse - The Place To Be

Policy Created:	February 2016
Policy Approved	Amended April 2018
Date of Next Review:	November 2025

Linked Policies/Procedures

1.	Data Protection, Archiving and Retention Policy

1. Vision and values

Wellhouse – the Place to Be.

This simple statement is our vision of Wellhouse as an attractive place where people feel happy and safe, benefit from having a good home and an attractive environment and feel proud to be part of a vibrant community.

We believe that our values of Trust, Honesty and Integrity, Excellence, Accountability and Sustainability supported by a comprehensive policy framework will help make our vision a reality.

2. Governance

Wellhouse HA is a community controlled registered social landlord and is managed by a group of people who are elected onto the Management Committee. Their role is to make sure that the Association is well run, meets the needs of the local area and is responsive to what is important to local people.

The Management Committee appoints senior staff, agrees all the Association's policies and takes all the key decisions. The Director and the senior team support the Committee with these responsibilities.

3. Policy Aims

This policy sets out the standards expected of Wellhouse Housing Associations employees, workers, governing body, stakeholders, consultants and agency staff when processing data whether that is in connection with Wellhouse Housing Association business or in the case of social media platforms the expression of views that contradict, oppose or infringe on the purpose, ethos or principles of Wellhouse Housing Association.

4. Equal Opportunities Statement

We aim to ensure that all services, including the delivery of this policy, provide equality of opportunity.

We will respond to the different needs and service requirements of individuals. We will not discriminate against any individual for any reason, including age, disability, gender re-assignment, marriage, civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation, or other status.

5. Introduction

Wellhouse Housing Association is committed to compliance with all statutory requirements, encompassed under data protection legislation, when handling, processing, storing and deleting information.

6. Principles

- This policy applies to all employees, workers, governing body members, stakeholders, consultants and agency staff of Wellhouse Housing Association and refers to the processing of data at Wellhouse Housing Association.

- Individual departments and administrative units may define separate categories of data under their supervision. Any such additional conditions must be consistent with this overall policy but may include more detailed guidelines and, where necessary and appropriate, additional restrictions.
- Any Wellhouse Housing Association employee or organisation which processes data on behalf of Wellhouse Housing Association consents to all of the provisions of this policy and agrees to comply with all of its terms and conditions and with all applicable laws and regulations.
- Any processor of data whose actions violate this policy or any other Wellhouse Housing Association policy or regulation, may be subject to disciplinary action in accordance with Wellhouse Housing Associations disciplinary procedures.
- The policy aims to ensure that processing of data among Wellhouse Housing Association employees and data processors is consistent with its own internal policies, all applicable legislation, and the individual user's job responsibilities.
- The policy also aims to establish basic guidelines for appropriate processing of data which comply with General Data Protection Regulations.

7. The Policy

General Data Protection Regulations Policy

Our Commitment

Wellhouse Housing Association is committed to provide equal opportunities across all services and avoid discrimination. This policy is intended to assist Wellhouse Housing Association to put this commitment into practice. Compliance with this policy should also ensure that employees do not commit unlawful acts of discrimination.

Contents

SECTION 1: INTRODUCTION

Wellhouse Housing Association is committed to compliance with all statutory requirements, encompassed under data protection legislation, when handling information.

Legislation relevant to this policy includes:

- Charities and Trustee Investment (Scotland) Act 2005;
- Human Rights Act 1998
- The Freedom of Information (Scotland) Act 2002
- The Environmental Information (Scotland) Regulations 2004
- The Companies Act 2006

The key legislation, referred to throughout this policy is:

- **The General Data Protection Regulation (EU) 2016/679**

SECTION 2 THE LAW AND GOOD PRACTICE

What is the General Data Protection Regulation?

The General Data Protection Regulation (EU) 2016/679 ("the GDPR") came into force on 25th May 2018 and replaced the 1998 Data Protection Act. It is designed to protect the privacy of individuals, in particular with regard to the processing of their personal information. Under the terms of the GDPR, "processing" data can mean obtaining, recording or holding the information or carrying out any operation or set of operations on the information including:

- Organisation, adaptation or
- alteration; Retrieval, consultation or
- use; Disclosure;
- Blocking, erasure or destruction; of the information or data.

The GDPR legitimises the processing of personal data. All processing activities require to be legitimised in terms of categories specified in the legislation. Failure to consider these categories prior to processing could result in the processing being unlawful.

Wellhouse Housing Association will adhere to the 8 principles of GDPR as recommended by the Information Commissioner, these being;

1. Processing personal data fairly and lawfully.
2. Processing personal data for specified purposes.
3. The amount of personal data an organisation may hold
4. Keeping personal data accurate and up-to-date
5. Retaining personal data
6. The rights of individuals
7. Information security.
8. Transferring personal data outside the EEA.

The GDPR is wide in scope and requires that all Organisations involved in the processing of data relating to living persons and personal data contained in some manual systems, be notified to the Office of the Information Commissioner (OIC). This covers for example, any personal data stored on desktop PC"s, laptops, memory sticks, CD Rom, DVD, mobile phones, PDAs and videotapes. Wellhouse Housing Association must ensure that all processing of data is accurate, up to date, and held for no longer than necessary. This means, for example, that when data becomes out of date or no longer relevant to the purpose for which it was originally obtained, it should be destroyed. The GDPR also sets out the rights of individuals and gives the Information Commissioner specific powers.

Wellhouse Housing Association

The GDPR gives individuals the right to see information about them held by Wellhouse Housing Association to have the information corrected or erased (the right to be forgotten) and in certain circumstances can prevent Wellhouse Housing Association from processing their details. It also means that if Wellhouse Housing Association causes them harm (physical or financial) or distress as a result of a breach of the GDPR they could claim compensation. Wellhouse Housing Association could also be prosecuted for serious offences.

Our Employees

Employees can also be prosecuted for unlawful action under the GDPR. This could result in a fine if they use or disclose information about other people without their consent or proper authorisation by Wellhouse Housing Association. Employees could also be committing an offence if they give information to another employee who does not need the details to carry out their legitimate Wellhouse Housing Association duties.

Due to the sensitivity of the data being processed by Wellhouse Housing Association, it is very important that all employees understand the need to abide by the eight principles set out in the GDPR.

The Principles are explained below: -

Personal data shall be:

- processed fairly and lawfully;
- obtained only for specified and lawful purposes and further processed only in a compatible manner;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- kept for no longer than necessary;
- processed in accordance with the rights of the data subjects;
- kept secure;
- Transferred outside the European Economic Area (EEA) only if there is adequate protection.

Wellhouse Housing Association will issue Fair Processing Notices to employees, tenants, owner occupiers, members and committee members on compliance with the legislation affecting the use of personal data and has complied with this policy in order to ensure that personal data is protected. Contractors, advisors and consultants will also be provided with the Fair processing Notice and will be expected to comply with similar policies and procedures when data is shared with them for the purposes of them carrying out services on behalf of Wellhouse Housing Association

Wellhouse Housing Association will ensure all data held electronically is secure and access is encrypted and/or password protected.

We will also ensure any paper documents stored for archive purposes are kept in a secure locked location, financial and legal information and all other types of information will be kept for a minimum period of time to adhere to statutory requirements but will be kept no longer than this unless there is a legitimate reason for doing so.

A SUMMARY OF THE KEY POINTS OF THE GDPR

- Manual records are covered by the GDPR. This relates to access to housing records
- Special category data has been introduced, which is broadly similar to sensitive personal data
- Data subjects have rights to object to the processing of personal data and the right to be forgotten and have wider compensation rights
- The transfer of personal data outside the European Economic Community Area is restricted
- Details of security precautions, both technical and organisation, require to be stated
- The Information Commissioner has increased powers.

The GDPR requires Wellhouse Housing Association to be pro-active in respect to:

- *The disclosure of personal data*
- *Personal information held in structured manual records*
- *Processing of sensitive data*
- *Data matching*
- *Security of personal data*
- *Retention policies*

Further information can be obtained from the Information Commissioner. It may also be helpful to access the Information Commissioner's web site www.ico.org.uk to keep up to date with legislation.

In Scotland there is a specific Information Commissioner at;
www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx

Who is Wellhouse Housing Association's Data Protection Officer?

Wellhouse Housing Association is registered with the Information Commissioner as a Data Controller.

- The Finance & Corporate Services Manager is the Data Protection Officer for Wellhouse Housing Association.

SECTION 3 THE GDPR PRINCIPLES

The eight Principles are detailed below.

1. Processing personal data fairly and lawfully The GDPR expressly provides that personal data is not to be treated as processed fairly unless, as far as practicable, certain conditions are met. These include informing data subjects of the identity of the Data Protection Officer and any nominated representative, as well as informing the data subject of the purpose(s) for which his/her data is to be processed. The only exceptions are where providing the information would involve disproportionate effort or where law requires recording or disclosing the data. The GDPR restricts usage to the following categories, some of which are clearly defined while others are capable of some interpretation. Processing may only be carried out where one of the following conditions has been satisfied:

- the individual has given consent to the processing
- the processing is necessary for the performance of a contract with the individual
- the processing is required under a legal obligation
- the processing is necessary to protect the vital interests of the individual
- the processing is necessary to carry out public functions
- the processing is necessary in order to pursue the legitimate interests of the business (unless prejudicial to the interests of the individual)

If you cannot justify the use of data in any of the above ways, you may be considered to be processing the data unfairly.

Stricter conditions apply to the processing of sensitive data. This special category data includes information relating to racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, health, sexual life and criminal convictions. The ***explicit*** consent of the individual will usually have to be obtained before sensitive data can be processed unless the controller can show that the processing is necessary based on one of the criteria laid out in the GDPR. This policy provides more detail regarding processing sensitive data later in section 4.

A Fair Processing Notice (FPN) must be provided to all individuals whose personal data is collected, at the outset of the collection of that data by Wellhouse Housing Association. Procedures will need to be developed to ensure that the FPN is issued alongside tenancy application packs and personal data contained within those applications is processed. It is recommended that a FPN is provided to all new tenants/factored owners. Wellhouse is under no obligation to ensure that the FPN has been read by the recipient.

The FPN must contain details of the following:-

- Contact details of the Data Controller and Data Protection Officer.
- Data processing purpose
- Recipients of the data
- Details of any transfer of the data out with the EU and the protections in place
- How long the data will be held, or if unknown, how the data controller will detrermine how long it is to be held
- Information on whether the data will be processed as part of an automated decision making process and the consequences of such processing

- Information on the data subjects rights including the consequences of their failure to provide such data where required by statute or contract
- Any further information which is not already covered by the above.

Data subjects have the right, at any time, to:-

- Ask for a copy of the information held about them by Wellhouse Housing Association
- Require Wellhouse to correct any inaccuracies in the information
- Make a request to Wellhouse to delete any personal data we hold about them (right to be forgotten).
- Object to receiving any marketing communications from Wellhouse

If departments intend to publish personal details or photographs on Wellhouse Housing Association's Web Site, the subject must give his or her informed and **written** permission.

2. Processing personal data for specified purposes. Processing of personal data must be registered with the OIC on an annual basis. The Data Protection Officer manages this on behalf of Wellhouse Housing Association. A copy of what is covered will be available on the Commissioner's Web Site (www.ico.org.uk) or from the Data Protection Officer. A standard template for data processing has been produced by the OIC, which is much simpler than the previous registration system. This is completed as part of the data mapping exercise. Only a general description is required of the processing of personal data being carried out. It is the responsibility of each Manager to ensure that the information contained in each category of data reflects and includes the processing which is carried out within individual departments.

Each department should regularly review the personal data they hold to ensure that the information in the data mapping exercise contains (a) particulars that adequately describe all processing of personal data; (b) a sufficient explanation of the reason(s) for which the personal data is held e.g. statutory powers; (c) the sources, disclosures and types of personal data If a potential discrepancy is identified between the data map and processing that might occur within a department, that should be brought to the attention of the Data Protection Officer as soon as possible.

All disclosures should be lawful and compatible with established procedures and notification entries. Personal data should only be disclosed after proper identification of the disclosee(s). All staff within each department should be made aware of the particular responsibilities pertaining to the disclosure of personal data and be properly trained to ensure that they do not disclose personal data without following established procedures.

3. The amount of personal data that is held. Departments should be able to justify why personal data is held and undertake to ensure that any item of personal data is within the scope of the data map. Each department should have established, and regularly review, procedures that check the relevance of personal data and be able to explain to data subjects why particular data is required. There are specific provisions relating to the retention of certain categories of data. Guidance on the retention periods for recorded material that includes personnel information can be found in the Code of Practice published by the Information Commissioner.

4. Ensure personal data is accurate and where necessary, kept up to date.

Departmental procedures will be in place to validate all personal data is up to date. The procedures will incorporate requirements for necessary corrections of personal data, to rectify

or erase such data as may be necessary and to advise disclosures of such changes whenever appropriate.

5. Retaining personal data for no longer than is necessary Departmental procedures will review the length of time that personal data is kept and monitor whether personal data is still required. This should take into account legislative requirements regarding retention periods of data. Personal data no longer needed should be deleted. Where personal data is kept for historical or statistical purposes, departments should be prepared to justify the grounds for this decision.. There are specific provisions relating to the retention of certain categories of data. Guidance on the retention periods for recorded material that includes personnel information can be found in the OIC Code of Practice.

6. The rights of individuals. The data subject is entitled to: - (a) a copy of any data processed by reference to him or her (b) a description of the data being processed (c) a description of the purposes for which it is being processed (d) any information as to the source of this data (where available) In addition, where the data is processed automatically and is likely to form the sole basis for any decision significantly affecting the data subject, then he/she will also be entitled to know the logic involved in that decision making.

It should be noted that back-up data and archived data is no longer exempt from subject access requests. Dependent on the level of subject access requests, this may be an area where there will be an increased cost implication, as archived systems tend not to be easily and cheaply searchable.

Personal data processed for: ***- the prevention or detection of crime - the apprehension of prosecution of offenders or - the assessment or collection of any tax or duty*** are exempt from the subject access provisions.

Personal data contained in confidential references, such as education/employment references, given by the Data Protection Officer are also exempt from subject access. Access to manual records that comprise of housing tenancy records are now covered by the GDPR.

7. Take security measures to prevent unauthorised accidental access to, alteration, disclosure or loss and destruction of information. Where processing is carried out by a data processor on behalf of Wellhouse Housing Association, Wellhouse Housing Association must choose a data processor that provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and take reasonable steps to ensure compliance with those measures. A data protection addendum will need to be completed and signed. The OIC is promoting following the guidelines of BS7799 Code of Practice for Information Security Management. Wellhouse Housing Association will not be regarded as complying, this principle unless the processing is carried out under a contract in writing under which the data processor is to act only on instructions from Wellhouse Housing Association. Departments should therefore identify who their processors are and ensure that appropriate data protection addendums/contracts are signed in accordance with the GDPR requirements.

8 Do not transfer personal data to a country or territory outside the European Economic Area unless there is an adequate level of protection for the rights and freedoms of the individual in relation to processing personal data. It should be noted that any personal information included on

Wellhouse Housing Association's Web pages comply with this principle.

The following are some of the exemptions to the transfer restrictions: (a) the data subject has given consent to the transfer (b) the transfer is necessary for the performance of a contract between the data subject and the data controller (c) the transfer is necessary for reasons of substantial public interest (d) the transfer is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings). (e) The information is on a public register

ACTIONS NECESSARY TO ENSURE COMPLIANCE

The following is a list of "compliance audit" actions that are necessary to ensure compliance with the GDPR. This list is not exhaustive and not specific to any particular service. It is not arranged in any particular order of priority.

1. Carry out an audit of all manual systems to determine where and how they are kept, which hold personal data and how the data is structured, accessed and processed.

2. Prepare a list of the purposes for which your department processes data (computerised and manual), the recipients and the sources of the data.

3. Identify all statutory purposes.

4. Identify (separately) the purposes for which you require to hold and process sensitive personal data items. Include both statutory and non-statutory reasons for requiring such data.

5. Perform an audit of existing security procedures to determine their adequacy and appropriateness, frequency of review and staff awareness. Where none exist introduce the necessary procedures including frequent reviews.

6. Establish procedures for identifying and recording data provided in confidence.

7. Establish procedures to deal with data subjects objections to the processing of personal data and to the disclosure of data which could reveal an individual as a third party source.

8. Check the existence of statutory retention periods: recommend periods: departmental policy.

9. Establish procedures to ensure compliance with the eight principles.

10. Establish procedures to deal with requests to disclose data to organisations that require it for the investigation or prosecution of offences, whether these are criminal, required by regulators or for the investigation of fraud.

11. Check to ensure that all personal data processing has been notified to the Information Commissioner.

12. Review standard forms to ensure that individuals are informed: (a) who will process their details (b) the purpose(s) for the collection of information (c) who the information will be disclosed to, if applicable.

13. Set up procedures to deal promptly with an individual's request to access their personal data.

14. Train and brief all relevant staff on the implications of the GDPR. Relevant refresher training should be provided a

15. Raise any queries or concerns regarding data retention, processing or responses to data subject requests with the Data Protection Officer.

CARRYING OUT A REGULAR COMPLIANCE AUDIT WILL HELP ENSURE THAT THE RISKS ASSOCIATED WITH THE USE OF PERSONAL DATA ARE WELL MANAGED.

SECTION 4: PROCESSING SPECIAL CATEGORY DATA

The DPA gives special protection to sensitive personal data. This is defined as data that relates to:

(a) an individual's race or ethnic origin
(b) health or sex life
(c) political or religious or other beliefs
(d) trade union membership
(e) criminal convictions, or allegations of criminal activity

Where sensitive personal data is concerned, the data subject must give his or her **"explicit" consent".** Guidance notes produced by the OIC states that for consent to be absolutely clear:

The data subject should be provided with:

(a) specific details of the processing
(b) the particular type of data to be processed
(c) The purposes of the processing and any special aspects of the processing.

Blanket consent for general data processing is unlikely to be sufficient for this type of data. It is essential to ensure that the data subjects are not misled as to Wellhouse Housing Association's reasons for requiring to process personal data and the legitimacy of any request.

Use of a tick box should be used with care as the OIC and the courts will not look kindly upon tick boxes that are ambiguously worded or worded so that consent can be implied from a failure to respond. **Informed explicit consent** should be obtained for sensitive data.

There will be occasions however, when providing too much information about the statutory purpose could be prejudicial and against the interests of the data subject or a third part, for example information which is entered on an "at risk register".

The only exemptions to obtaining explicit consent for processing sensitive data are detailed below:

- Required by law and is done so in connection with the employment of a data subject
- Protect the vital interests of the data subject or other person, where consent cannot be reasonably obtained or has been unreasonably withheld. (The Commissioner regards this condition as being applicable only „where processing is necessary for matters of life and death").
- Specific non-profit organisations, which exist for political, philosophical, religious or trade union purposes.

- The data has been made public by the deliberate actions of the data subject.
- Legal purposes
- Administration of justice, exercise of functions established by law or required by the Crown, Ministers of the Crown or of government departments.
- Processing by an “anti-fraud” organisation that furthers the purposes of fraud prevention.
- Medical purposes and undertaken by a Health Professional or someone with an equivalent duty of confidentially.
- Monitoring equality of opportunity and treatment of racial or ethnic groups with a view to promoting equality and provided there are appropriate safeguards.

Where a Wellhouse Housing Association department obtains information of a confidential nature in order to carry out its statutory functions then processes that information for other purposes, there is likely to be a breach of the obligation of confidence to that individual, unless there is a good reason or some legal justification for using the information in that way.

All departments should check their existing systems, both manual and automated, to determine the extent to which they hold such sensitive data; whether or not such data is relevant for (Housing Association)’s purposes; if they have a statutory right to process such data; to determine if they need the consent of the data subject etc.
In any case, departments wishing to hold and process sensitive data should always seek the subject’s consent and provide him/her with details of the purpose(s) for which it is required including any statutory purposes.

The following are guidelines on processing sensitive data produced by the Personnel Policy Research Unit on behalf of the Office of the Data Protection Commissioner.

1. Trade Unions

You should not process data about individual employee’s membership of a trade union without the consent of each employee concerned. This includes the practice of recording union membership on payroll systems for the purpose of deducting regular subscriptions.

2. Criminal Records

2.1 Employers shall not process any personal data concerning the alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by any employee unless they have a right to do so under Employment Law, or the data is necessary for the purpose of, or in connection with, any actual or potential legal proceedings.

2.2 Employers have the right to request, process data about an employee’s criminal record in accordance with the terms of The Police Act 1997, providing that it does not involve the infringement of an individual’s rights under The Rehabilitation of Offenders 1974.

2.3 Data held about particular convictions on an employee’s criminal record should be automatically removed from an employer’s files as soon as the conviction is legally „spent“, unless the employee concerned is in an exempt occupation under The Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975. Personal data relating to an employee’s criminal record should not be passed onto any third party without the prior, explicit consent of the employee concerned.

2.4 Employers must not require or encourage any individual to supply them with copies of, or material from, their criminal records (either directly or via a third party) by utilising their individual data access rights, unless the employer has a statutory right or duty to do so.

3. Employee Testing

3.1 Employers should not require employees to undergo genetic testing (or other tests identifying susceptibility to disease) unless it can be objectively justified on either strong public, or employee, health and safety grounds. Such test may be carried out with the prior consent of the employee concerned and if the results are interpreted by a qualified health professional.

3.2 Alcohol and drugs testing in the workplace must be carried out with the prior informed consent of the employees concerned, be a clear element of their individual employment contracts and form part of an explicit health information, education and rehabilitation policy

SECTION 5: DISCLOSURE OF PERSONAL DATA

Disclosures to outside organisations, including the police and other agencies, should only be undertaken by properly trained and authorised personnel.

In general, a disclosure must only take place (subject to the eight principles of the GDPR) if one of the following conditions applies:

- The individual has given consent to the disclosure;
- It is a legal obligation, for example requests made by the Inland Revenue, Council Benefit Fraud teams and DWP under their statutory powers or by order of the Court;
- Disclosure is necessary for: (i) prevention or detection of crime; (ii) the apprehension or prosecution of offenders; or (iii) the assessment or collection of any tax or duty so long as Wellhouse Housing Association can prove that it had reasonable grounds for believing that failure to make the disclosure in question would be likely to prejudice any of the above.

A Data Protection Officer should be clear about whether they have a **POWER** or a **DUTY** to disclose. You may have a power to disclose but not a duty, therefore you could refuse to disclose personal information on the basis of maintaining the confidentiality of a third party. Any disclosure of personal data must have regard to both common law and statute, for example defamation, the common law duty of confidence and the data protection principles, subject to any exemptions which apply. The GDPR principles set out above must also be complied with.

When requests for personal data are received on the telephone, staff should be advised not to disclose any personal data unless authorised to do so from their line manager. Even where approval has been given, staff should not disclose information over the telephone before the caller's identity has been verified (e.g. by phoning them back on a known number, or by confirming a known reference number, or by discussing some reference details known only to the caller). This may be difficult if the caller is agitated or angry but usually callers will divulge information that will help to assess their true identity.

If common sense suggests that a particular disclosure should be an exception to Wellhouse Housing Association's procedures (e.g. where someone might be at risk, or a risk) staff should

be trained to consult their line manager and make a proper record of the disclosure, to whom it was made and the circumstances that made it necessary.

Disclosures to the Police

Section 29(3) of the DPA allows disclosure of personal data if (1) the data is to be processed for the purposes of prevention or detection of crime or the apprehension or prosecution of offenders and (2) non-disclosure would be likely to prejudice those purposes.

When disclosing information to the police under Section 29(3) it is Wellhouse Housing Association and not the Police, who must be reasonably convinced that failure to disclose would prejudice the enquiry. The Information Commissioner has stated that
"*there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged"*

What you need to obtain from the police are details of:

(a) the crime being investigated;
(b) the reason for the enquiry (i.e. the appropriate GDPR exemption purpose);
(c) how the absence of any information would be likely to prejudice the enquiry.

The police generally use a standard form to request the disclosure of information. It should be noted that this form is only a request for information

If you have any reservations, and if you do not wish to provide the data, you should ask the police for a court order. If you disclose information without satisfying yourself that the exemption is valid you are in breach of the GDPR.

Disclosures to Government Agencies

The GDPR also allows disclosure of personal data if (1) the data is to be processed for the purposes of assessment or collection of any tax or duty or similar matter, and (2) non-disclosure would be likely to prejudice those purposes. Requests for these purposes should be treated in the same way as those from the police.

Inland Revenue and VAT Inspectors will often additionally refer to the relevant section of the GDPR (which provides that personal data may be disclosed where the disclosure is required by or under any enactment, by any rule of law or by the order of a court), stating that they are acting under their statutory powers.

If any government body, whether Inland Revenue, VAT Inspectors or otherwise, quotes the correct section of the GDPR and provides a section number or paragraph number from a relevant statute – that is insufficient unless it is also accompanied by the relevant statutory wording relied upon.

Disclosures to other Departments

Staff should ensure that any disclosures of information to other Wellhouse Housing Association Departments are fair and lawful. To be lawful you need to ensure that the request meets at

least one of the conditions for data processing, contained in the GDPR (as summarised at Section 3 above, GDPR principle 1).

Information obtained for one purpose, cannot be used for another purpose without the knowledge and consent of the individual concerned. The exception to this is if a department has the power to ask for this information under other legislation.

Disclosures to Committee Members

The common law principles governing Wellhouse Housing Association's Committee members are summarised below:

(a) A Committee member, by virtue of his/her office, is entitled to have access to all documents in possession of Wellhouse Housing Association as far as access is reasonably necessary to enable him/her properly to perform his/her duties.

(b) A Committee Member has no „roving commission" in respect of Wellhouse Housing Association documents and mere curiosity is not a sufficient basis for access to information.

(c) In the case of a Committee of which the Committee Member is a member, there is a presumption that the Committee Member has good reasons for access to all the information and documents which pertain to the functions of that particular Committee.

(d) In the case of a Committee of which the Committee Member is not a member, he/she has no automatic right of access to material and has to demonstrate a "need to know".

Personal data disclosed to Committee Members remains the property of Wellhouse Housing Association and cannot be used or disclosed for purposes other than those contained in Wellhouse Housing Association's Data Map. Any use of the data, for purposes other than those of Wellhouse Housing Association, could result in the Committee Member and/or Wellhouse Housing Association acting ultra vires (outwith their powers), breaching confidence and committing an offence under the GDPR.

Committee Members acting on behalf of individual tenants or applicants may be expected to demonstrate that they are doing so, and should obtain the tenant or applicant's written consent. Then, when requesting access to personal data about that individual they should present such consent as proof.

Refusing to disclose Personal Data

Where disclosure of data is refused, staff should be polite and explain that they are not allowed to disclose personal data unless the caller's credentials to receive the data have first been verified. Staff should always explain the reason why they are refusing to give information is one of confidentiality and because the caller has not provided adequate identification. It could also be that the personal data is exempt from disclosure to a particular party under the GDPR.

Emergencies

There may be circumstances where staff have to disclose personal data in emergencies. If an emergency involves a threat to a data subject's health or if it will prevent injury to a data subject then the disclosure can take place.

A proper record of the disclosure must be made, either at the time, or as soon as possible after the disclosure has occurred. In other urgent situations, staff will have to use their judgement but in all cases they should keep a formal record of their decision to disclose and send a note of the disclosure to their line manager.

Requests to other public bodies for information

Other public authorities and organisations have their own data protection obligations and disclosure procedures as a result of the GDPR. Therefore, when dealing with other organisations Wellhouse Housing Association should be aware that the GDPR, as well as other legal obligations of confidentiality, may restrict the information that any other organisation can provide to Wellhouse Housing Association.

SECTION 6: INFORMATION SHARING

Checklist for Information Sharing (Multi-Agency Teams)

Legislation has enabled information sharing between agencies, including the Social Security Administration Act 1992 (as amended), under which RSLs are allowed (and, in some cases, required) to share information in respect of benefit claims and with other agencies to match data for the purposes of preventing and detecting benefit fraud. Also, the Crime and Disorder Act 1998 (Section 115) allows Wellhouse Housing Association to share information where the disclosure is necessary or expedient for the purposes of any provision of that Act – however, those purposes are restricted and care should be taken when a request for sharing is made under this provision alone. Additionally, it should be noted that such legislation may provide a lawful basis on which information may be shared, but Wellhouse Housing Association will need to consider whether other legal obligations are owed to individuals in relation to the personal data they hold, e.g. duty of confidence.

The following is a suggested checklist for setting up information sharing arrangements within Wellhouse Housing Association.

What is the purpose of the information sharing arrangement?

It is important in data protection terms, that the purpose or objective of any information sharing arrangement is clearly defined. If personal data is to be shared, then the disclosures must be notified to the Information Commissioner.

Is it necessary for personal data to be shared in order to fulfil that purpose?

If depersonalised information can be used to achieve the purposes of the arrangement, then there will be no data protection implications.

Do the parties to the arrangement have the power to share or disclose personal data for that purpose?

If it is decided that the objectives of the information-sharing arrangement could not be achieved without sharing personal data, then each party to the arrangement will need to consider whether they have the power to share or disclose information for the purpose of the arrangement. If Wellhouse Housing Association acts outside its powers it will be acting illegally.

What personal data needs to be shared in order to achieve the objectives of the arrangement?

Consideration must be given to the extent of personal data that is disclosed. It may be that an individual has come to the attention of an agency, which through their involvement with that individual holds a wide range of information on that individual. But disclosure of all that personal data may not be relevant to the purpose for which the information sharing arrangement has been established. This is a matter for consideration by each agency holding information about an individual.

Has the consent of the individual been sought before the disclosure is made?

Consideration must be given to whether the information can be disclosed lawfully and fairly.

There is a non-disclosure exemption in the GDPR which provides that information may be disclosed for the purposes of prevention and detection of crime or the apprehension and prosecution of offenders, where failure to disclose would be likely to prejudice those objectives.

Many of the data protection issues surrounding disclosure can be avoided if the consent of the individual has been sought. This is particularly significant if the personal data to be shared identified victims of, or witnesses to, incidents.

What if consent of the individual has not been sought or has been sought but has been withheld?

Consideration must be given to whether the information can be disclosed lawfully and fairly.

To assist staff, there is a written protocol relating to the sharing of information with MPs, MSPs and Committee Members who may enquire of Wellhouse Housing Association on behalf of a constituent, tenant or other individual. This protocol ensures that they are clear as to their responsibilities and liabilities.

SECTION 7: SUBJECT ACCESS

As well as imposing obligations on Wellhouse Housing Association, the GDPR gives enhanced rights to individuals about whom information is held, including rights to seek compensation for breaches of the DPA.

An individual who makes a subject access request to Wellhouse Housing Association is entitled:

- To be told whether Wellhouse Housing Association holds any personal data relating to that individual, *and*
- To be supplied with a copy of all the information that forms any such personal data

Requests for subject access should be made in writing to the Data Protection Officer and accompanied by the appropriate access fee. Wellhouse Housing Association has prepared a standard subject access form, but it may have to be amended, dependent on the service department. The standard form is only an aid to identify the personal data requested and Wellhouse Housing Association has no legal right to insist that it is completed.

The Data Protection Officer will monitor all subject access requests. On receipt of a subject access request the Data Protection Officer will progress the request as detailed below:

(a) The identity of the data subject will be verified. This should be thorough and appropriate to the sensitivity of the data;

(b) Ensure that the necessary information is supplied to locate the personal information requested;

(c) once all checks are satisfactory, the Data Protection Officer will proceed with the request and advise the data subject that Wellhouse Housing Association is processing the subject access request and that a copy of personal data held by Wellhouse Housing Association, subject to exemptions, will be provided within 1 month;

(d) The appropriate departments will be contacted and asked to check their records for any personal information related to the data subject and forward a copy to the Data Protection Officer. When processing subject access request, departments should have a clear methodology for accessing the personal data as this information may be required for audit purposes should an appeal be raised. It will not be acceptable to say that all files have been checked and no records found. It is very important that there is an audit trail should further investigation be required;

(e) On receipt of the data, all printouts, files etc., will be checked to ensure that they can be understood and any codes explained;

(f) Where applicable, third parties will be contacted to gain their consent prior to disclosing information where they could be identified. This is particularly relevant where individuals ask for access to „accessible records" such as manual tenancy records;

(g) Where necessary, any references to third parties (those identifiable as living individuals) will be blocked or erased unless explicit permission has been granted to disclose;

(h) All information supplied will be checked for any exemptions under the GDPR;

(I) all information being disclosed to the data subject will be photo-copied;

(j) Once completed, the Data Controller will write to the data subject supplying all information (within 1 month);

(k) The data subject will be advised if no data is held or if the data is subject to any exemptions under the GDPR;

(l) On receipt of the information, the data subject may ask for information to be corrected. The Data Protection Officer will investigate the complaint and, if substantiated, will arrange for the data to be amended/deleted (as appropriate) by the member of staff responsible for the data held;

(m) Any complaints made to the OIC will be investigated by the Data Protection Officer.

It should be noted that neither the verification nor the time taken should be excessive and once satisfied, procedures must allow for a copy of the data subjects data to be provided to them within **1 month.** Wellhouse Housing Association is not obliged to comply with a subject access request unless the request is in writing, the appropriate fee has been received, the necessary information is provided to enable the authority to identify the person making the request and to locate the personal information. This timeframe is legally binding.

It is essential that all staff that receive a subject access request recognise it as such and immediately notifies the Data Protection Officer.

INFORMATION RELATING TO ANOTHER INDIVIDUAL

A particular problem arises for departments who may find that in complying with a subject access request they will disclose information relating to an individual other than the data subject, who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of the information. The GDPR recognises this problem and sets out only two circumstances where Wellhouse Housing Association is obliged to comply with the subject access request;

- Where the other individual has consented to the disclosure of the information, or
- Where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

Where it is not reasonable to disclose information regarding third parties, their names and details should be deleted from the relevant documents prior to sending to the data subject.

For further information regarding third party information please refer to the leaflet produced by OIC entitled “Subject Access Rights and Third Party Information”.

SUBJECT ACCESS REQUEST MADE ON BEHALF OF CHILDREN

All individuals have the right to make subject access requests. In relation to the capacity of a child to make subject access request, a child under 16 may exercise any right under the GDPR when he or she has a general understanding of what it means to exercise that right and a person of 12 years or more shall be presumed to be of sufficient age and maturity to have such understanding.

Accordingly, when Wellhouse Housing Association receives a subject access request from a child there will need to be a judgement on whether or not the child understands the nature of the request.

If the child does not understand the nature of the request, someone with parental responsibilities for the child, or a guardian, is entitled to make the request on behalf of the child and to receive the response.

SUBJECT ACCESS TO PERSONAL DATA CONTAINED IN EMAILS

Some emails contain personal data but fall outside the scope of the GDPR since those data were not processed by reference to the data subject. An example may be a reference to an individual in the minutes of a meeting, which are kept as a record of the meeting. Others will clearly fall within the scope of the GDPR, for instance where the name of the data subject appears in the title of the email or she/he is the sender or the recipient.

For further information please refer to guidance issued by the Information Commissioner.

DATA SUBJECT"S RIGHTS UNDER THE GDPR

- A right of access to personal data
- A right to prevent processing likely to cause damage or distress
- A right to be forgotten
- A right to prevent processing for purposes of direct marketing
- Rights in relation to automated decision making including the right to have logic explained

The data subject is entitled to:

- A copy of any data processed by reference to them
- A description of the data being processed
- A description of the purposes for which it is being processed
- A description of any potential recipients of their data
- Any information as to the source of their data (where available)

If personal data is held only for preparing statistics or carrying out research, and it is not used or disclosed for any other purpose and if the results of the research are not disclosed in any way which identifies the data subjects, then the subjects do not have a statutory right of access to the data. However, it is still good practice to give them a copy of their data if they ask for it.

RECTIFICATION, BLOCKING, ERASURE AND DESTRUCTION

The data subject may apply to the Court for an order requiring the Data Controller to rectify, block, erase or destroy such data relating to them, as is inaccurate, as well as any other personal data which contains an expression of opinion which the court finds is based on the inaccurate data. Data will be inaccurate if incorrect or misleading as to any matter of fact.

A court may also make such an order if it is satisfied, on the application of a data subject, that they have suffered damage by reason of any contravention by a Data Controller of any of the requirements of the their in respect of personal data, entitling them to compensation and that there is a substantial risk of further contravention in respect of that data in such circumstances.

RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS

An individual is entitled to serve upon a Data Controller a written notice requiring the Data Controller to cease or not to process personal data of which that individual is the data subject, where such processing is causing or is likely to cause unwarranted substantial damage or substantial distress to them or to another.

The Data Controller has 21 days to respond to the data subject by way of a written notice to the individual stating that the Data Controller has complied, or intends to comply, with the data subject notice or stating their reasons for regarding the data subject notice as, to any extent,

unjustified. Where the data subject considers that the Data Controller has not complied with a data subject notice they can seek a court order. If the court agrees it can order the Data Controller to take such steps as are necessary to comply with the notice.

RIGHTS TO PREVENT PROCESSING FOR PURPOSES OF DIRECT MARKETING

An individual is entitled, by written notice, to require a Data Controller to cease or not to begin processing personal data relating to that individual for the purposes of direct marketing and may apply to court for an order to that effect if the Data Controller fails to comply with the notice

The GDPR defines direct marketing as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This includes arrangements to insert details of other organisations products/services in communications addressed to individuals, including payslips, or where lists of names and addresses are sold to third parties for marketing purposes.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING

An individual is entitled, by written notice, to require a Data Controller to ensure that no decision which significantly affects them is based solely on the processing by automatic means of personal data of which that individual is the data subject. For example, performance monitoring, automatic CV scanning and an individual's creditworthiness.

RIGHT TO COMPENSATION

An individual who suffers damage or damage and distress as the result of any contravention of the requirements of the GDPR by a Data Controller is entitled to compensation where the Data Controller is unable to prove that they have taken such care as was reasonable in all circumstances to comply with the relevant requirement.

Therefore, compliance with this policy and departmental procedures linked to this policy will assist Wellhouse Housing Association to address claims should individuals exercise their rights and seek compensation due to alleged unlawful disclosure.

ANNEX TO SECTION 7: Standard Form for Subject Access Request

Wellhouse Housing Association
The General Data Protection Regulation (EU) 2016/679
SUBJECT ACCESS REQUEST

Under the terms of the General Data Protection Regulation (EU) 2016/679, an individual is entitled to ask Wellhouse Housing Association for a copy of all their personal information which it holds.
All subject access requests must be made in writing and accompanied by the appropriate access fee. The request must also contain sufficient information as is necessary to enable Wellhouse Housing Association to identify the person making the request and to locate the personal information sought.

The completion of this form is voluntary and is only an aid to assist Wellhouse Housing Association in locating your personal data.

Name: .....

Address: .....

.....
.
Postcode: .....

Date of Birth: .....

National Insurance Number: .....

Length of time at this address: .....

If you have lived at this address for less than two years, please give details of your previous address.

Previous address: .....

.....

Post Code: .....

Length of time at that address: .....

Type of Information Sought

You are entitled to access all your personal information held by Wellhouse Housing Association, subject to any exemptions which apply under legislation. However, to assist us in locating any specific information you require, it would be helpful if you could indicate the areas in which you are interested.

1. I am requesting access to the following personal information held by (Housing Association):

Tenancies ☐
House Waiting List ☐
Repairs & Maintenance ☐
Employment Record ☐
Other (please give details) ☐

2. Access to specific personal information (please give details)

.....

.....

Data Subject Declaration

In exercising the right granted to me under the terms of the General Data Protection Regulation (EU) 2016/679, I request that you provide me with a copy of the personal data about me which you process for the purposes I have indicated above.

I confirm that the aforementioned is all of the personal data to which I am requesting access and which is held by Wellhouse Housing Association for its purposes. I also confirm that I am the data subject and not someone acting on his/her behalf.

Signed ..... Date .....

This section to be completed by person(s) acting on behalf of the data subject.

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

Name .....

Address .....

.....

Post Code .....

Signed ..... Date .....

Wellhouse Housing Association
SUBJECT ACCESS FEE

Under legislation, Wellhouse Housing Association has the right to charge a fee for access to personal information. Although we will commence with the collection of information upon receipt of confirmation to proceed. Where it deemed that the level of work involved to collate and provide the information is significant, the information will not be released until the fee has been paid.

Access Fee

Subject Access Request under the Data Protection Act 1998

Name: .....

Address: .....

.....

Post Code: .....

Please find enclosed the appropriate access fee to enable Wellhouse Housing Association to proceed with a formal subject access request.

Access Fee under Data Protection Act 1998 enclosed

SECTION 8: EXEMPTIONS

There are a number of exemptions from various provisions of the GDPR, referred to as "the primary exemptions", and those referred to as "the miscellaneous exemptions". In general, the primary exemptions are the ones which are either more likely to be applicable or which are more wide-ranging in terms of the scope of the exemption available.

If you have any queries regarding whether an exemption might apply in a particular case, the matter should be raised first with your line manager and, if not resolved, thereafter with the relevant Data Protection Officer.

PRIMARY EXEMPTIONS

a) Safeguarding National Security

If required for the purpose of safeguarding national security, personal data are exempt from any of the Data Protection Principles.

b) Crime and Taxation

The DPA contains three categories of exemption which may be claimed under this heading:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of any tax or duty or any imposition of a similar nature

c) Health, Education and Social Work

There are specific regulations regarding exemptions relating to:

- Personal data as to the physical or mental health or condition of the data subject
- Personal data relating to present or past pupils or schools
- Personal data designated by the Secretary of State and which appear to him / her to be processed in the course of or for the purposes of carrying out social work in relation to the data subject or other individuals.

In the case of the social work exemption there is a proviso in the GDPR that the Secretary of State shall not grant any exemption or make any modification unless he/she considers that not to do so would be likely to prejudice the carrying out of social work.

d) Research, History and Statistics

An exemption applies where:

- The data are not processed to support measures or decisions relating to particular individuals, and
- The data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

e) Disclosures required by law

Where the disclosure is required by or under any enactment, by any rule of law or by the order of a court, personal data is exempt from the non-disclosure provisions.

(f) Disclosures made in connection with legal proceedings

Where the disclosure is necessary:

- For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings).
- For the purpose of obtaining legal advice, or,
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights, personal data are exempt from the non-disclosure provisions.

MISCELLANEOUS EXEMPTIONS

(a) Confidential references in respect of employment, training, education or the appointment to office or provision of any service are exempt from subject access. It should be noted that this exemption is not available for such references where they are received by the data controller

(b) Management forecasts/management planning

(c) Corporate Finance

(d) Negotiations: personal data recording Wellhouse Housing Association's intentions in relation to any negotiations with a data subject are exempt from subject access provisions to the extent to which access would be likely to prejudice those negotiations.

(e) Examination Marks

(f) Examination Scripts

(g) Legal professional privilege

SECTION 9: SECURITY OF PERSONAL DATA

The GDPR expands on security requirements by explicitly stating what precautions data users must take. Technical and organisational measures must be taken to prevent the unauthorised or unlawful processing or disclosure of data.

There is also a requirement for Wellhouse Housing Association to ensure that where work is given to an independent processor there is a written contract between the parties, this is known as a data protection addendum. The contract should include a clause that states the processor agrees only to act on the instructions of the Data Controller and to abide with the provisions of the security principle. Wellhouse Housing Association must choose a processor with care i.e. one with sufficient guarantees of good practice within technical organisational security and also meets all Wellhouse Housing Association's ethical standards requirements.

Committee Members and all employees of Wellhouse Housing Association dealing in any way with personal data must take all possible precautions to protect data against unauthorised loss,

destruction or disclosure. All employees should adhere to Wellhouse Housing Association's Information Security Policy.

All employees dealing with data should be told the purpose(s) and disclosure(s) which have been notified to the OIC and reminded that the use of the data for any other purpose(s) or unauthorised disclosure(s), even if accidental, may constitute an offence under the GDPR.

In accordance with the GDPR, BS7799 certification (Code of Practice for Information Security Management) would provide a good indication that an organisation has endeavoured to take „due care" in safeguarding the security of its information. The principle of due care is an important element of the GDPR, and certification will have a key role to play in future policy decisions and contract negotiations with third parties. Wellhouse Housing Association has based their information security policy on the key controls contained in BS7799 and seeks to work towards accreditation.

Procedure Review Questions to consider when reviewing security precautions for your department

(a) Physical Security

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

(b) Software Security

- How is access to equipment, programmes and personal data restricted to appropriate staff?
- How sensitive are the data?
- How is password security maintained?
- How regular are access and usage monitored?

(c) Printed Matter

- Where are documents (e.g. computer printouts) stored?
- How is computer output disposed of?
- How is access to documentation controlled?

(d) Staff Awareness

- What precautions are taken to prevent accidental disclosures?
- Are staff aware of security issues and Wellhouse Housing Association's security policy?
- What security training have staff received?
- Who is responsible for the security of personal data?

(e) Contracts

- Do contractors, external agents or consultants have in their contract a written obligation towards the requirements of the GDPR?

SECTION 10: MANUAL FILES

Personal data held in structured manual files will be covered by the GDPR. „Structured files" means any set of information relating to individuals to the extent that it is filed either by

reference to individuals or by reference to criteria relating to individuals in such a way that the information is “readily accessible”. Readily accessible files can be a „grey area‟ so Data Controllers should err on the side of caution. If there are individual names on the front of the cover they should assume that files are caught by the GDPR.

The key definition is not about „relevant filing systems‟ but „personal data‟. The data protection principles require personal data to be processed fairly and lawfully; for specific purposes; be adequate, relevant and not excessive in relation to its purpose; accurate and (where necessary) kept up to date and not stored for longer than is necessary. To comply with all these requirements Wellhouse Housing Association will not be able to hold ANY data about identifiable individuals outside the full and direct control of the GDPR.

The following are examples of manual files, which will be caught by the GDPR:

a) card index systems
b) housing records
c) HR files

Manual files that will not be caught by the GDPR are for example, Policy files and Housing Property files which include general information about the property.

All structured manual files should be reviewed to ensure that they do not contain any inappropriate data or inappropriate comments about the individual.

It will be necessary, in respect of manually processed data, therefore for departments to demonstrate that the conditions required under the principles are being met:

- The date subject has given consent to disclosures
- Use of the data is covered by statute
- No items of sensitive personal data is processed unless explicit consent has been obtained
- Adequate security measures are in place
- Details of sources of, and organisations to which, data will be disclosed are maintained
- Retention periods are known and observed.

A Data Controller will have to:

a) Put procedures in place to deal with an individual’s right to prevent processing in certain circumstances.

b) Be able to destroy, erase or block data which are shown to be inaccurate.

c) Ensure that staff are fully aware of their duties and responsibilities.

d) Determine whether or not the files are structured within the definition as contained in the GDPR.

In the longer term it is likely that it will be easier to comply with the GDPR if the retention of manual records is reduced to a minimum.

SECTION 11: DATA MATCHING

Data matching exercises designed to assist in the detection of fraud are widely in operation throughout the public sector. The term „data matching" essentially means the comparison of data collected by different data users, (or by the same data user in different contexts). The aim of the comparison is not primarily the creation of a larger file of information about the data subject but the identification of anomalies and inconsistencies within single set or data or between two or more different sets. These sets of data will often be derived from application forms. Systems are designed to produce indicators of possible fraud for further investigation and not to take decisions about the validity of particular applications.

Exercises of this sort raise privacy concerns in that although the majority of applicants for benefits, goods or services are honest and there is no prior indication of any wrongdoing on their part, data relating to them is to be shared and scrutinised by a range of other organisations. This loss of privacy has led some people to warn of the capacity of the data matching exercises to reverse the normal rules of evidence and the presumption of innocence and to raise fears of the use of computer technology to conduct mass surveillance of the population.

According to the Information Commissioner:

"wholesale data matching exercises are a major invasion of the private lives of people to whom no suspicion of any wrongdoing attaches. In passing the Fraud Act, Parliament has set down clear rules as to the circumstances under which their data may be matched. Employees have the right to expect that their employers will keep their personal data securely and not disclose them unless required to do so by law".

The Social Security Administration (Fraud) Act 1997 amended the Social Security Administration Act 1992 to provide the Department of Work and Pensions (DWP) with a statutory basis on which gain access to information on the two social security benefits, Housing Benefit and Council Tax Benefit, which are administered by local authorities. Although Wellhouse Housing Association is independent of the DWP, the law allows Wellhouse Housing Association to supply information on these benefits to the DWP for data matching purposes. However, Wellhouse Housing Association must comply with the law with regard to data protection.

The use of data matching exercises for other purposes should comply with the data protection guidelines to ensure data is not processed unlawfully. Any proposed data matching exercises which include HR records etc., should involve full consultation with staff and, if necessary, amendments to Terms and Conditions of Employment and/or Code of Conduct.

Data matching must be carried out within a specified timeframe to avoid data becoming out of date and therefore inaccurate

Copy of the guidelines can be obtained from Wellhouse Housing Association's Data Protection Officer. As yet, there is no statutory Code of Practice for matching.

SECTION 12: NOTIFICATION

The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller (via the web site – www.ico.org.uk). Notification is the process by which a data controller's details are added to the register.

The notification entry has to be renewed on an annual basis.

Section 13 : Policy Review

We ensure that this data protection policy is reviewed on a 3 yearly basis.