1. HOMES FOR WELLS GDPR DATA PROTECTION POLICY

This policy sets out Homes for Wells' (HFW) General Data Protection Regulation (GDPR) policy, and applies to all personal data we hold for any identifiable person. We will do our best to make sure that personal data held on past, present and future tenants will be handled sensitively and confidentially by all staff, agents and members of our board and committees. This policy also covers past, present and future staff, shareholders, donors, directors and volunteers or contractors who work with us from time to time, and others with whom we have dealings. We recognise the need to treat personal data in an appropriate and lawful manner.

Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Acts, and the General Data Protection Regulations (GDPR). These acts and regulations impose restrictions on how we may use personal data.

2. POLICY STATEMENT

This policy should be read together with our Privacy Information Notice. HFW will act with integrity and comply with the six Data Protection Principles to hold and process personal data:

lawfully, fairly and transparently
for specified, explicit and legitimate purposes
ensuring that it is adequate, relevant and limited to what is necessary for these purposes
keeping data accurate, relevant and up to date
for no longer than is necessary for our purposes as stated in our Privacy Information Notice
in a manner which ensures security, protection, integrity and confidentiality
and the Data Controller shall be accountable for compliance with these principles

All staff, board and committee members and agents must comply with this policy and our internal procedures as well as the GDPR. In doing so, they will:

Treat all personal and sensitive data as confidential, and correct it if is shown to be inaccurate

Comply with the law regarding protection and disclosure and not disclose information without the prior informed consent of the individual concerned, except in the circumstances detailed below under 'Disclosure' or where otherwise required by law.

Not try to gain access to information they are not authorised to have.

Keep data no longer than necessary, and destroy it when no longer required, in line with best practice and retention rules

Securely protect data against loss or disclosure and in accordance with the GDPR and our Privacy Information Notice and make data available to the data subject on request

This policy may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action against employees. In the event that the policy is breached by any director, volunteer, contractor or agent we may require them to undertake more specific training in personal data handling if they wish to remain involved with HFW.

3. STATUS OF THIS POLICY

This policy has been approved by the HFW Board. It sets out our rules on data protection and legal conditions that must be satisfied in the relation to the obtaining, handling, processing, storage, transportation and destruction of personal data.

The Data Controller shall be responsible for,and be able to demonstrate compliance with the Data Protection Acts and GDPR. The Data Controller is Roderick Day who can be contacted by calling (01328) 711203 or by emailing rod@homesforwells.co.uk. Any questions or concerns about the operation of this policy should be referred first to the Data Controller.

If you consider that this policy has not been followed, whether in respect of personal data about yourself or about others, you should raise the matter immediately with the Data Controller. A breach could have very grave consequences for an individual or HFW, and will be treated as a very serious matter. Disciplinary action, including dismissal in a serious case, will be taken against any employee of HFW who commits a breach of this policy. HFW may also be open to criminal proceedings that may result in an unlimited fine or criminal proceedings.

4. DEFINITION OF DATA PROTECTION TERMS

Personal data is information which is stored electronically, on a computer or in certain paper-based filing systems and means any information relating to an identified or identifiable person (data subject) who can be identified by reference to a name, an identification number, location data, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. All data subjects have legal rights in relation to their personal data. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as whether an individual is suitable as a tenant for a particular property).

Data Controllers are the people who determine the purposes for which and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Acts and the GDPR. Data Controllers must be able to demonstrate compliance with data protection principles, and all their general obligations under the GDPR. They must:

- be accountable, and keep a detailed record of processing operations
- Perform data protection impact assessments for high risk processing if applicable
- Notify, record and report any data breaches
- Implement data protection

- HFW‘s records must include:
- The name and contact details of the Data Controller
- The purposes of the processing
- A description of the categories of data subjects, and of the categories of personal data
- The categories of recipients to whom the personal data has has been or will be disclosed
- The time limits for destruction of different categories of data
- A general description of the technical and organisational security measures

Data subjects include all individuals about whom we hold personal data. Data subjects have legal rights in relation to their personal data.

Data Processors include any person who processes personal data on behalf of a Data Controller. Employees of data controllers are excluded from this definition. Data Processors must maintain proper documentation, cooperate with the ICO, implement appropriate security standards and notify data breaches to the Data Controller.

Data Users include staff whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data or carrying out any alteration or set of operations on the data including organising, amending, retrieving, using, erasing or destroying data.

Sensitive personal data includes information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, or information about the commission of, proceedings for, offences committed or alleged to have been committed by that person. Sensitive personal data can only be processed under strictly limited conditions and will usually require the express consent of the person concerned.

5. OBJECTIVES

to ensure compliance with GDPR and data protection rules on confidentiality

To make sure all staff and board members of HFW are aware of and understand the importance of data protection and confidentiality

To protect the personal and sensitive information of staff, tenants, board members, shareholders and donors

To make sure tenants are able to access their own information within the time limits

Each year to review the disclosure categories as part of our internal systems

To make sure procedures are in place for staff, contractors and board and committee members on disclosure of personal information

To make sure all staff receive appropriate training with regular updates whenever there are changes to the guidance

6. ACCESS TO INFORMATION AND DISCLOSURE OUTSIDE HFW

HFW employees will generally have access to all the information they need to carry out their work, and they have a duty to keep that information confidential.

In the unusual event that any information must be disclosed to someone outside HFW, staff must explain to the data subject why this is necessary and obtain written consent before doing so. If the data subject does not give consent, this should be noted and special arrangement should be made for recording information and access to it. However, relevant agreements and protocols are in place that allow for the exchange of information between HFW and the relevant local authorities in relation to to the processing of housing applications and in the prevention of crime and antisocial behaviour. There are certain situations where the law says that HFW do not have to obtain prior consent to disclose personal data about individuals. These are:

- To comply with the law (for example police, Inland Revenue, council tax registration or a court order)
- Where there is a health and safety risk (this will include information about tenants with a history of violence and when other care professionals are involved in a customer's care).
- Where there is evidence of fraud.
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions (for example applications for possession, or for paying housing benefit directly).
- Where the name of the tenant and the date of occupancy is given to utility companies (where the tenant is responsible for direct payment), providing the tenant has agreed to this at the start of the tenancy or it is a condition of the tenancy agreement, or the tenant has given consent to the passing on of the information.
- To allow anonymous inclusion in official statistical reporting, or for research purposes, providing it is not possible to identify the data subject to whom the information relates
- Where specifically required by the terms of the GDPR.
- Where there are declarations of interest by staff, committee or board members.
- Where there may be concerns about a tenant regarding safeguarding of adults from abuse, or related concerns regarding safeguarding children.

- If it is necessary to discuss individual tenants at meetings involving people from outside HFW or to refer to them and reports, they will be referred to by code numbers and anonymised to maintain confidentiality.

7. DATA RETENTION AND DISPOSAL

Personal data will be destroyed as soon as practicable when it is no longer needed. The method of disposal should be appropriate to the confidentiality of the information. However the law requires for certain documentation to be retained permanently or for six years after the end of the contract, and HFW will act in accordance with the retention of documents for housing associations rules. For example, a tenancy file and agreement will be kept for six years from the end of the tenancy and then destroyed.

8. DATA SUBJECT RIGHTS

The GDPR built on the current rules by enhancing existing data subject's rights and adding a number of entirely new data subject's rights. These include:

- The right to rectification of personal data
- The right of subject access to personal data
- The right to restrict processing of personal data
- The right to object to processing of personal data
- The rights not to be subject to automated decision taking, including profiling
- The right to transparency
- The right to data portability

The right in some circumstances to erasure of personal data (the right to be forgotten) if there is no compelling contractual or legal reason for its continued processing.

9. DATA SECURITY

Personal data should not be shared informally. The only people who may access it it those who are authorised and legitimately need it for their work.

HFW must ensure that all appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may complain to the ICO or apply to the courts for compensation if they have suffered damage from such a loss.

The law requires us to put in place procedures and technology to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

(a) **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(b) **Methods of disposal**. Paper documents should be shredded. Hard disks, floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

(c) **Equipment.** Data users should ensure that any laptop or PC used is password protected and that mobile equipment including laptops, smart phones and USB sticks are never left unattended or unprotected in the presence of third parties.

10. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them can be made verbally or in writing. This does not include data about any other person. Anyone who receives a written request should forward it to the Data Controller immediately. HFW should respond within 28 days but in certain cases this can be extended to 3 months. HFW all keep a record of all such requests.

11. PROVIDING INFORMATION OVER THE TELEPHONE

Anyone dealing with telephone enquiries should be extremely careful about disclosing

any personal data held by us. In particular they should:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) Refer to the Data Controller for assistance in difficult situations. No-one should be bullied into disclosing personal data.

If there is any doubt, the rule is not to disclose any personal data at all.

12. MONITORING AND REVIEW OF THE POLICY

This policy is reviewed annually by our board and may be updated from time to time. We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.