Data Protection Policy

Document Control							
Valid from	Valid to	Version	Status	Author(s)	Owner	Approval	Description of change
Dec 2012	Dec 2015	1.0	Final	Information Officer	Group Director of Finance	FHG Board 11.12.12	New Policy
Oct 2015	Oct 2016					Exec Team approved 1 year extension	None
Oct 2016	March 2018					Group Directors Approved extension due to impending new legislation	None
May 2018	May 2021	2.0	Final	Risk & Compliance Manager	Group Finance & Resources Director	FHG Board 22/5/18	Major overhaul to reflect requirements to comply with GDPR
Feb 2019	Feb 2022	2.1	Final	"	"	EPB Feb 2019	Minor changes only
Distribution/confidentiality				All team members, temporary and agency staff			
Other relevant documents:				Data Breach Management Policy Data Breach Management Procedure Data Breach Management Process Map Data Retention Policy Data Subject Rights Leaflet FHG Privacy Notice – Overview FHG Privacy Notice – Full Fraud & Financial Crimes Policy Privacy Impact Assessment Template Subject Access Request Procedure General Data Protection Regulation 2018 Information Governance Forum - Terms of Reference Disciplinary Policy & Procedure *ISMS - ICT Security Policy [pending approval]* *ISMS - Acceptable Use Policy [pending approval]* Standing Orders & Financial Regulations Whistleblowing Policy & Procedure Code of Conduct for Board Directors Code of Conduct for Team Members Agile Working Policy Probity Policy			

Contents

1 DEFINITIONS

1.1 **Personally Identifiable Information**: any information which relates to an identified or identifiable natural person, for example, an individual's name, date of birth or contact details. For the purposes of this policy, personal data also includes special category data (see 1.2 below).

1.2 **Special Category Data**: these are special categories which specifically relate to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

1.3 **Privacy Notice**: Under the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018 ('DPA'), individuals have the right to be informed about how their personal data is being used. This is documented and communicated through a Privacy Notice and in a clear, transparent and unambiguous manner.

1.4 **Data breach**: A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of or access to personal data. A data breach extends beyond losing personal data, for example it includes sharing personal data with the wrong person.

1.5 **Data Processor**: Responsible for processing personal data on behalf of a data controller. The GDPR and DPA place specific legal obligations on a data processor for example, a requirement to maintain records of personal data and processing activities and a legal liability if found to be responsible for a data breach.

1.6 **Data Controller**: Responsible for determining the purposes and means of processing personal data. The GDPR and DPA place obligations on a Data Controller to ensure that contracts with data processors comply with the GDPR and DPA. Under the GDPR Article 5(2), the data controller will be responsible for and be able to demonstrate compliance with the data protection principles (as defined in section 5 below).

2 POLICY STATEMENT

2.1 Futures Housing Group ('the Group'), including its subsidiary companies, is committed to protecting the personal and special categories of data which it processes in accordance with all applicable data protection laws and regulations and in a fair and transparent manner.

2.2 Legal and regulatory safeguards impose restrictions on how personal and special category data may be processed.

2.3 This policy applies to and must be adhered to by the Group's Board Directors, Committee Members, employees (including temporary / agency staff) and third parties (whether current or past processors). The policy applies in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data relating to its customers, suppliers, employees and other third party contacts ('data subjects').

2.4 This policy applies to all processing of personal data in electronic form (including email, IP Addresses, biometrics) and where it is held and as structured data in manual files.

3 ACCOUNTABILITY

3.1 Where the Group collects and uses personal data and makes decisions about its use, it will act as the Data Controller and take responsibility for how that data is collected and used. In such cases, the Group recognises its responsibility for ensuring compliance with this policy and for demonstrating compliance with the GDPR and DPA.

3.2 It is recognised that non-compliance with this policy may expose the Group to complaints, regulatory action, substantial fines and/or reputational damage.

3.3 The Board and Group Directors are fully committed to ensuring the effective implementation of this policy and expect all Board Members, employees, temporary and agency staff and third parties (whether current or past processors) to comply fully with the policy. Any breach of this policy will be taken seriously and may result in disciplinary action.

4 RESPONSIBILITIES

4.1 Those referred to in section 3.3 are expected to manage personal data in a professional and ethical manner and in line with the Group's Codes of Conduct. The Board will oversee the Group's strategic management of data protection.

4.2 The Group Audit and Risk Committee will seek independent assurance over the adequacy and effectiveness of the Group's data protection arrangements. This will include monitoring the Group's management of data protection risk and using the internal audit plan to assess compliance against applicable data protection laws and regulations.

4.3 The Group's Information Governance Forum ('IGF') has responsibility for overseeing the development and delivery of the Information Governance programme. This includes, overseeing policy implementation and promoting an effective security and compliance environment. IGF responsibilities are defined further within the IGF Terms of Reference.

4.4 The Group Finance and Resources Director acts as IGF Chair and has overall responsibility for ensuring that all personal data processed by the Group is managed in line with this policy. The Board and Group Audit and Risk Committee will be notified of any significant deviation(s) from this policy. The Group Finance and Resources Director will also work in conjunction with the Data Protection Manager to ensure that the Group responds in a proportionate way to any information breaches that may arise including, where appropriate, reporting to the Board and Information Commissioners Office ('ICO').

4.5 The Co-Executive Team will oversee the Group's operational management of data protection and ensure that all service lines comply fully with this policy. It will also ensure that appropriate controls, safeguards and processes are designed and operate effectively to minimise the Group's risk exposure in relation to data protection.

4.6 All Group employees managing personal data on the Group's behalf are expected to do so in a professional and ethical manner and in line with the Group's Code of Conduct for Team Members. Employees must inform their line manager and the Data Protection Manager as soon as they become aware of data loss, data being deleted, processed or amended without authority or a breach of confidentiality regarding

personal data. Employees can report concerns through the Group's Data Breach Policy and Whistleblowing Policy.

4.7 Employees must not discuss personal or confidential data with anybody who has no right to know, including other employees and third parties. They will also keep such data secure from visitors, other employees and contractors who do not need access to the information in order to carry out their duties.

4.8 Where there is a requirement to discuss personal data internally, this will be done in private and only between employees who have a legitimate right to access that information in order to carry out their duties.

4.9 Third parties who act as data processors on the Group's behalf must acquaint themselves with and comply with this policy and terms agreed through their contracts and signed deeds of variation to their contracts. They must also complete GDPR/DPA position surveys as appropriate. The Group will not engage with any third parties who do not comply with this policy or their contractual terms regarding data protection.

4.10 The Data Protection Manager will act as Secretary and Deputy Chair of the IGF and will inform the Group of any changes to data protection laws and regulations, advising the Group on designing appropriate processes to enable compliance with this policy and prevailing laws and regulations. The Data Protection Manager will support the Group Finance and Resources Director in reporting any significant deviation(s) from this policy or data breaches to the Group Chief Executive, Board and Group Audit and Risk Committee. They will also support the Group in delivering training to maintain a strong data protection culture amongst employees and third parties.

5 DATA PROTECTION PRINCIPLES

5.1 The General Data Protection Regulation ('GDPR') Article 5 defines several principles to govern the processing (i.e. collection, use, retention, transfer, disclosure and destruction) of personal data. These principles require personal data to be:

1) *Processed lawfully, fairly and transparently in relation to data subject ('lawfulness, fairness and transparency');*

2) *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4) Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be

processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); and

6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Controller must also be able to demonstrate compliance.

6 RIGHTS OF DATA SUBJECTS

6.1 Under the GDPR and DPA an individual (data subject) has eight rights. The Group as a Data Controller will comply with these rights. Employees and third parties processing data for the Group must understand and preserve these rights for the benefit of the Group's customers and other employees.

6.2 The Group has documented the rights in its Leaflet on Data Subject Rights which is available on their website, and these cover the following:

- Right to be informed;
- Right to access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability;
- Right to object; and
- Automated decision making.

7 DATA PRIVACY

7.1 The Group will not ask for information that is unnecessary for the purpose it is being collected. It has documented a Privacy Notice which defines what personal identifiable information it collects, how it is used, with whom it is shared and how it is secured. The Privacy Notice also explains an individual's privacy rights. This is available on the Group's website.

7.2 The Group recognises the importance of maintaining high standards with regard to data integrity and privacy. This extends to amending or introducing new processes and systems to ensure continued compliance with data protection laws and regulation.

7.3 The Group requires the data controller of any process or system which is being updated or replaced to ensure that such revisions comply with relevant data protection laws and regulations. Therefore, employees and third parties acting as data controllers must complete a Data Privacy Impact Assessment ('DPIA') for all new systems and processes and for any revisions to existing systems and processes

which contain personal data. The DPIA enables data controllers to assess how personal data and associated risks will be managed during process / system change.

8 DATA RETENTION

8.1 The Group has a Data Retention Policy which defines:

- responsibilities for managing data retention;
- retention periods;
- considerations for retaining / disposing of data; and
- requirements for disposing of data securely.

8.2 The Data Retention Policy applies to anyone processing information on behalf of the Group. All Board Members, employees, temporary and agency staff and third parties are expected to comply fully with the Data Retention Policy.

9 INFORMATION ASSET REGISTER

9.1 The Group documents all of its personal data and purposes in an Information Asset Register ('IAR').

9.2 Managers will inform the Data Protection Manager of any changes to personal data being held in the systems / processes which they operate to enable the IAR to be updated with accurate and up to date information. The Governance and Compliance team have responsibility for maintaining the IAR.

10 DATA BREACH MANAGEMENT

10.1 The Group is legally required to report all personal data breaches to the ICO within 72 hours of becoming aware of the breach. Failure to notify a breach to the ICO can result in a fine of up to €10m or 2% of global turnover.

10.2 The Group has defined its framework for managing and responding to instances of unauthorised or unlawful processing regarding data loss, destruction or damage. Requirements are defined within the Group's Data Breach Management Policy and supporting Data Breach Management Procedure and Process Map.

10.3 The Data Breach Management Policy defines roles and responsibilities for managing, reporting and responding to data breaches. The Data Breach Management Procedure and Process Map provide guidance on identifying, investigating, reporting and recording a data breach.

10.4 All Board Directors, Committee Members, employees (including temporary / agency staff) and third parties (whether current or past processors) are expected to read, understand and follow the Data Breach Management Policy, Procedure and Process Map and any breach of these will be taken seriously and may result in disciplinary action.

11 SUBJECT ACCESS REQUESTS

11.1 The Group operates a Subject Access Request Procedure which must be followed whenever a request for personal information is received from an individual / data subject. The Group will process all requests in line with data protection legislation.

11.2 The Subject Access Request Procedure includes guidance on the processes to be followed by the Governance and Compliance Team. It includes requirements for confirming the identity of the data subject, preparing and checking information and disclosure considerations.

12 CCTV

12.1 The Group may undertake surveillance of its offices and properties using CCTV to prevent and detect crime against its people and assets and support law enforcement.

12.2 The Group's Privacy Notice includes details of where the Group's CCTV devices are located and the purposes for which the data are used. All CCTV will comply with the ICO's guide 'CCTV Data Protection Code of Practice'. This will include the use of appropriately sized signs informing of the presence of CCTV, the purpose of using CCTV and the contact details for the Assets Projects Manager (responsible officer).

12.3 As the Group is not a public body, there is no requirement for the Group to comply with the Regulation of Investigatory Powers Act 2000.

13 DATA PROTECTION TRAINING

13.1 Data Protection training is mandatory for all new starters at the Group and will be delivered as part of their induction. In addition, current employees must undertake annual refresher training in order to maintain awareness of current data protection laws and regulations and the Group's policies and procedures.

14 NOTIFICATION

14.1 An annual notification is submitted by the Group Finance and Resources Director to the ICO to advise what and how personal data is processed.

14.2 The Group's ICO registration numbers are as follows:

- Futures Housing Group Limited: Z1720721
- Five Doorways Homes Limited: Z2587857
- Futures Homescape Limited: Z7118710
- Futures Homeway Limited: Z1721653
- Futures Greenscape Limited: ZA382706
- Limehouse Developments Limited: ZA382458
- Futures Finance Limited: ZA501802
- Futures Treasury Plc: ZA501669

15 DATA PROTECTION CONTACTS

15.1 For general enquiries about the Group's Data Protection Policy and for formal subject access requests under GDPR, please email the Data Protection Manager at dataprotection@futureshg.co.uk

15.2 The Group's Mandatory Data Protection Officer ('MDPO') is the Data Protection Manager.

16 REVIEW

16.1 This policy will be reviewed on a three year basis or earlier in the event of a significant change to UK data protection legislation or regulation.