Data Protection Policy

If you need this publication in larger print, audio form, Braille, or in another language, please contact our office and we will try to help you.

KINGDOM HOUSING GROUP

DATA PROTECTION POLICY

1. Statement of Intent

1.1 This policy covers Kingdom Housing Association Limited and our subsidiary company Kingdom Initiatives Limited.

1.2 We are committed to the principles of good corporate governance and sustainability and will endeavour to develop fair and consistent policies, procedures and practices.

1.3 We recognise that data protection is important to protect the rights of individuals in respect to any personal information that is kept about them, whether on computer or in structured manual system.

1.4 Both Kingdom Housing Association Limited and Kingdom Initiatives Limited are registered with the Information Commissioner as Data Controllers.

1.5 The aim of this policy is to ensure that we comply with legislation which governs all policies where we intend to collate, handle, retain and destroy data.

1.6 Procedures have been developed and implemented to ensure compliance with this policy.

1.7 This policy also aims to raise the awareness of the need to manage data in accordance with the principles of data protection (see Section 2).

1.8 In line with our commitment to equality and diversity, this policy can be made available in a variety of formats, including large print, translated into another language or other media. We will make any reasonable adjustments to assist you if you have a disability.

2. Principles of Data Protection

2.1 **Personal data shall be processed fairly,** therefore we must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure we do not do anything unlawful with the data.

2.2 **Personal data shall be obtained only for one or more specified and lawful purposes,** therefore we must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it;
- comply with fair processing requirements – including our duty to give privacy notices to individuals when collecting their personal data;
- comply with notifying the Information Commissioner; and
- ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

2.3 **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed**, therefore we will ensure that:

- we hold personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual; and
- we do not hold more information than we need for that purpose.

2.4 **Personal data shall be accurate and, where necessary, kept up to date**, therefore we will:

- take reasonable steps to ensure the accuracy of any personal data we obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

2.5 **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**, therefore we will:

- review the length of time we keep personal data;
- consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

2.6 **Personal data shall be processed in accordance with the rights of data subjects**, therefore an individual has:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

2.7 **Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**, therefore we will:

- design and organise our security to fit the nature of the personal data we hold and the harm that may result from a security breach;
- be clear about who in our organisation is responsible for ensuring information security;
- make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

2.8 **Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**, therefore we will:

- consider sending personal data outside the EEA, by using a checklist devised by the Information Commission to help us decide if this principle applies and, if so, how we will comply with it.

2.9 A list of definitions referred to in legislation is attached as Appendix 1.

3. General Principles

3.1 This policy applies to all:

- Employees (for the purpose of this policy, employees include bank and agency workers, volunteers and those on placement).
- Appointed Agents and Contractors.
- Kingdom Housing Association Limited, Committee of Management.
- Kingdom Initiatives Limited Directors.

Data Processing

3.2 All data/information processed by both organisations is covered by this policy.

3.3 We will only process personal data where the data subject has given consent. Details of the reasons why the data is sought and the reasons for which it will be used will be stated on all forms as outlined in Appendix 2(a).

3.4 The processing of sensitive personal data will only be carried out with the individual's explicit consent as outlined in Appendix 2(b).

Third Parties

3.5 We may from time to time use reputable third parties for the processing of data and we will take all reasonable steps to ensure that such data is processed in accordance with this policy.

3.6 Data which has been provided to us, **in confidence**, by a third party such as employment references or tenancy reports cannot normally be disclosed to the data subject, unless the author of the data (third party) can remain anonymous or it is reasonable to comply with the access request without the author's consent.

Subject Access Requests

3.7 If we hold personal data on an individual, they have the right to access the information, unless it is exempt under legislation. A Subject Access Request flowchart is attached at Appendix 3.

3.8 Where we receive a request for information (this must be in writing, including email correspondence), we will respond within 40 days.

3.9 We will not normally charge for requests for information. However, we reserve the right to make a charge of up to £10 to cover administration, stationery and postage costs for repeated requests. The Committee of Management and the Directors of Kingdom Initiatives authorises Kingdom's Senior Management Team to apply this charge.

Security of Data (Retention and Disposal)

3.10 We are responsible for ensuring that any personal data (on others) which we hold is kept securely and that we do not disclose to any unauthorised third party.

3.11 All personal data will be accessible only to those who need to use it. Judgement will be based upon the sensitivity and value of the information in question, but we will always consider keeping personal data:

a) in a lockable room with controlled access;
b) in a locked drawer or filing cabinet;
c) if computerised, password protected; or
d) kept on storage media which are themselves kept securely.

3.12 We will ensure that display screens and terminals are not visible except to authorised staff and that our ITC passwords are kept confidential. Our display screen will not be left unattended without password protected screen savers and manual records will not be left where they can be accessed by others.

3.13 We will take care to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records will be shredded or disposed of as "confidential waste".

3.14 The IT Manager will be responsible for ensuring our IT Security Policy is applied and managed to protect data held on our ITC systems.

3.15 Managers have a responsibility to ensure generally that data within their department is protected on our ITC systems and manual records.

3.16 Where you have the authority to take data off-site, for example working from home, you are responsible for ensuring all data, whether the data is held on your ITC equipment or in a manual file, is protected at all times from unauthorised access.

3.17 Where you travel between sites or other locations, you are responsible for the security of this data, whether this is held on your ITC equipment or in a manual file, and the data is protected at all times from unauthorised access.

3.18 You may ask if you can use your personal hand held device(s) (such as smart phones, tablets and laptops) for work purposes. Likewise, we may make the same request to you. Management and employee guidelines have been prepared to determine whether, by using your own personal hand held device(s) to carry out your day to day duties, that data is protected at all times from authorised access. Our IT Security Policy will also apply.

3.19 Departments will regularly review what data they will dispose of in accordance with their departmental data auditing procedures.

3.20 We will dispose of personal data in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Close Circuit Television (CCTV)

3.21 We will use CCTV and other systems for reasons of personal security and to protect our premises and the property of staff and service users.

3.22 We will:

a) Complete an impact assessment to ensure our compliance with any legislation or code of practice (see Appendix 4).
b) Display signage to confirm CCTV is in operation.
c) Identify clearly defined and specific purposes for the use of images, and communicate to those who operate the system.
d) Clearly document procedures for how the images will be handled in practice.
e) Identify a limited number of authorised individuals who will have specific responsibility for the control, reviewing and destruction of CCTV imaging. These individuals will maintain confidentiality in respect of personal data.
f) Ensure proactive checks or audits are carried out on a regular basis to ensure that procedures are being complied with. These checks will be recorded and retained by authorised individuals.
g) Authorised individuals will review on an annual basis whether the use of CCTV continues to be justified.

3.23 We will not use or share images outwith our organisation (the Kingdom Housing Group) unless a criminal act has occurred, whether this is to you, a service user or a member of the public. Where a criminal act has occurred, upon request, we will provide the Police with the image(s) and they will become the Data Controller for the image(s) provided. We will normally decline other requests for copies of images.

Personal Safety

3.24 In order to protect the safety of our employees, we may consider using voice recording software, in addition to CCTV recording. The usage of this software and any associated equipment will be in compliance with this policy and our Data Protection Register Entry.

Committee of Management/Director of Kingdom Initiatives

3.25 If you are a member of the Committee of Management or Director of Kingdom Initiatives and you receive an enquiry from tenants or other customers, in respect of personal and/or sensitive data, you will advise the person to contact the appropriate member of staff rather than deal with enquiries yourself.

Internal Audit

3.26 An audit of this policy and associated procedures will be incorporated into the internal audit function of Kingdom.

Awareness Training

3.27 The Resources Department will arrange awareness training on Data Protection as follows:

a) Existing Staff – Awareness sessions were arranged for all staff following approval of this policy and associated procedures. Copies of this policy and associated procedures were issued to all staff with copies also contained within the Employee Handbook and on the network;
b) New Staff – Awareness training will be provided at the Organisational Induction.
c) The Committee of Management/Directors of Kingdom Initiatives Limited – members of the Committee of Management are encouraged to attend the awareness training arranged for existing staff and are also issued with this policy and associated procedure. New members of the Committee of Management/Directors of Kingdom Initiatives Limited are provided with awareness training as part of their induction process;
d) Appointed Agents and Contractors – any contractor or agent employed directly or indirectly by Kingdom will sign a confidentiality (non-disclosure) agreement before being granted access to data/information. This will include those on a paid or unpaid placement with us. A standard confidentiality (non disclosure) form is attached as Appendix 5 to this policy.

Whistleblowing

3.28 This policy will in no way affect the rights of disclosure of information under the Public Interest Disclosure Act 1998.

4. Responsibilities for Compliance

All Departments

4.1 It will be the responsibility of each of the Departmental Directors to ensure that this policy and associated procedures are applied within their own department.

4.2 Each Departmental Director has specific responsibilities for personal and sensitive information held on data subjects within their department.

4.3 Each Department will have a member (or members) of staff who have the specific responsibility for:

a) Auditing data;
b) Checking data for quality, consistency and duplication of personal data within their department;
c) Promoting security of personal data;
d) Promoting the Data Protection principles in the Department;
e) Reviewing the registration criteria within their department and advising the Resources Director of any proposed amendments on an annual basis or more often if required;
f) Processing data subject access requests within their own department, in accordance with the agreed procedure;
g) Reviewing the retention periods of data.
h) Responding and co-ordinating requests from employees to access personal information we hold about them.

4.4 Each department will review the method of collecting data and will obtain the express consent of the data subject to process sensitive data.

Resources Department

4.5 The Resources Manager will be responsible for the following:

a) Notification and registering with the Information Commissioner;
b) Co-ordinating any amendments to Kingdom Housing Association Limited's or Kingdom Initiatives Limited's registration;
c) Ensure subsequent requirements for registration are complied with and will liaise with the Senior Management Team on the content of the registration.
d) Monitoring and reporting to the Senior Management Team and the Committee of Management/Directors of Kingdom Initiatives Limited on compliance of subject access rights;
e) Preparing and co-ordinating audit procedures;
f) Reporting findings of the Audit to the Senior Management Team and Committee of Management, if required;
g) Arranging identified and agreed training;
h) Review of the policy within an agreed timescale;
i) Liaison with the Information Commissioner as required.

4.6 The Resources Manager will assist in implementing the requirements of the Act by:
a) Providing advice and support to all departments on all matters relating to compliance with the Act;
b) Disseminating information relating to the Act;
c) Responding and co-ordinating requests from employees to access personal information we hold about them.

5. Breaches of Policy

Employees

5.1 If an employee knowingly breaches any aspect of this policy, this will be grounds for disciplinary action in accordance with our Disciplinary Policy and Procedure. Where you seriously breach this policy, a potential sanction may be dismissal.

Committee of Management/Directors of Kingdom Initiatives

5.2 If a Committee Member knowingly breaches the conditions of this policy this will be dealt with under our Policy and Procedures on Dealing with Breaches of the Committee of Management Code of Conduct. Any breach will also be reportable to the Information Commissioners Office and the Scottish Housing Regulator as a Notifiable Event.

5.3 If a Director of Kingdom Initiatives breaches the conditions of this policy this will reported to the Information Commissioners Office.

Agents and Contractors

5.4 If an Agent or Contractor knowingly breaches any aspect of this policy, this will be grounds for us reviewing their continued working relationship with us. Where they are on our approved list of consultants, contractors and suppliers, we may consider temporarily suspending any work they do whilst we carry out an investigation.

6. Monitoring and Review

6.1 Although the Resources Director and Resources Manager can advise the relevant manager on individual cases, it is the relevant manager who will make decisions relating to this policy and its associated policies.

6.2 On an annual basis prior to re-registration with the Information Commissioner, each Departmental Director will be provided with a copy of Kingdom Housing's registration requesting that this be reviewed with any proposed amendments incorporated into the registration. The updated registration form will be submitted to the Committee of Management seeking their approval prior to submission to the Commissioner.

6.3 On an annual basis prior to re-registration with the Information Commissioner, each Director of Kingdom Initiatives will be provided with a copy of Kingdom Initiative's registration requesting that this be reviewed with any proposed amendments incorporated into the registration. The updated registration form will be submitted to

the Directors of Kingdom Initiatives seeking their approval prior to submission to the Commissioner.

6.4 On an annual basis details of the number of subject access requests and whether or not these access requests have been arranged within the time period set out by the Data Protection Act will be reported to the Committee of Management and Directors if Kingdom Initiatives.

6.5 This policy will be reviewed 5 years from the date of implementation or latest review, which will be the date the policy is approved by the Committee of Management/Board of Directors, or earlier if deemed appropriate. In the event that this policy is not reviewed within the above timescale, the latest approved policy will continue to apply.

APPENDIX 1

DATA PROTECTION DEFINITIONS

Data Controller – Kingdom Housing Association Limited and Kingdom Initiatives Limited are the data controllers not individual staff members. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data Subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data Processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data (including manual data/relevant filing system) – information which:

a) is being processed by means of equipment operating automatically in response to instruction given for that purpose,
b) is recorded with the intention that it will be processed by means of such equipment;
c) is recorded as part (or with the intention that it will form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured, whether by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible); and
d) does not fall within paragraph a), b), or c) but forms part of an accessible record as defined in Section 68 of the Act.

Relevant Filing System is defined as:

"Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."

As a broad rule, we consider that a relevant filing system exists where records relating to individuals are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. Examples include:

a) Personnel Files – applications forms, staff performance and development reviews, disciplinary records, supervision notes etc;
b) Housing Records – application forms, waiting lists, rent accounts, etc;
c) Card indices – lists of names and addresses, contact numbers etc. and
d) Contacts which are retained on the ITC systems.

Accessible Record is defined as:

a) an accessible public record that consists of information held by a local authority for housing or social services purposes.

Personal Data data which relate to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data means personal data consisting of information as to:

a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether an individual is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by the individual of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

APPENDIX 2 (a)

DATA PROTECTION STATEMENT

We will use the information you give in this form, and in any supporting evidence you send us, to process your …… (define purpose i.e. application for housing)…… We may pass the information to other agencies or organisations as allowed by the law and in accordance with our Registration with the Information Commissioner.

Kingdom is registered under the Data Protection Act with the office of the Information Commissioner. Kingdom Housing Association Limited is the Data Controller for the purposes of the Data Protection Act.

As the Data Subject you have the right to access the information we hold on you. If you wish to exercise this right please contact our office and ask for a Data Subject Access Request Form.

APPENDIX 2 (b)

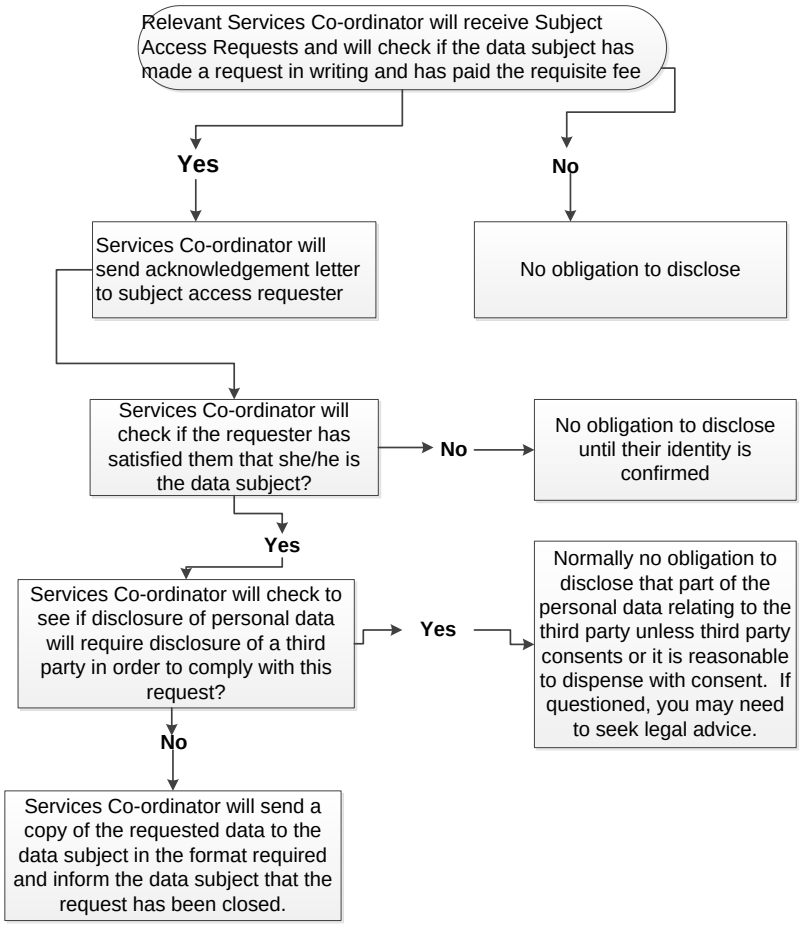
DATA SUBJECT EXPRESS CONSENT

In accordance with the Data Protection Act, information which is provided by you, which is defined as sensitive e.g. racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, mental or physical health, sex life, criminal records or allegations of criminal conduct, requires your express consent to enable us to process this information.

It is therefore essential that you sign the form where indicated to confirm you are aware of the need for us to collect this information and to confirm your permission for this.

I would be interested in hearing about any special arrangements or offers that might be available to me and others in connection with my tenancy e.g. special insurance offers.

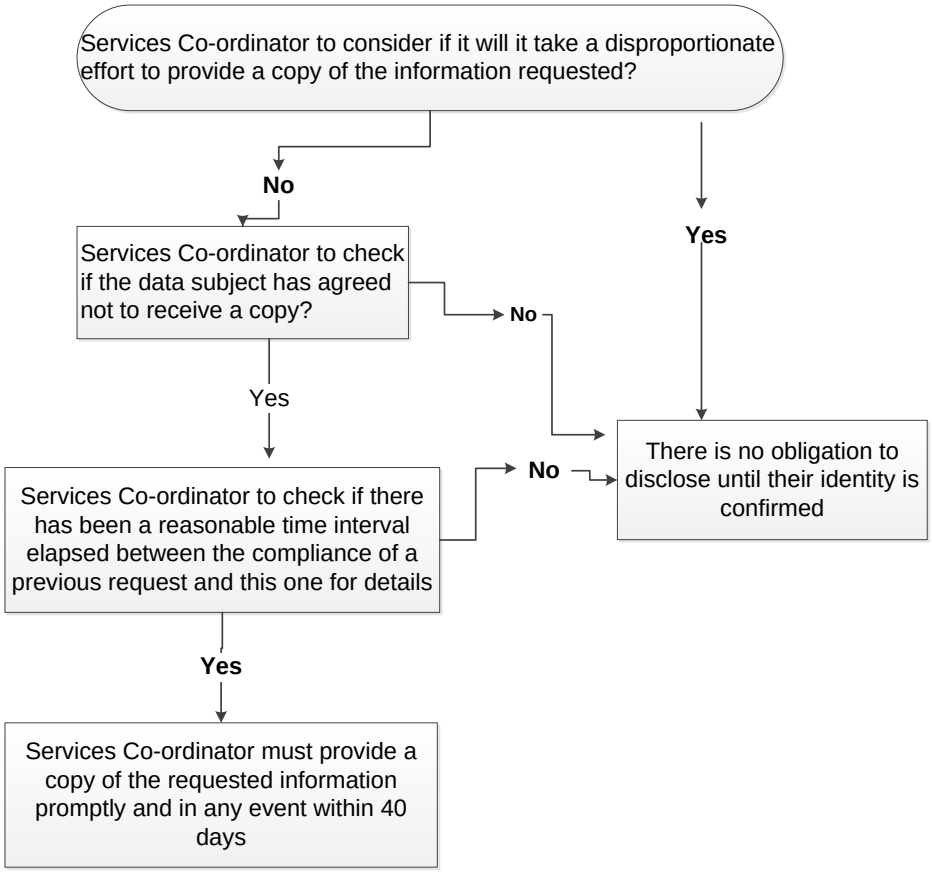
Please tick if interested: ☐



Remember: You have 40 days to respond to the request

METHOD OF PROVIDING INFORMATION CONTAINED IN A REQUEST — APPENDIX 4 (b)

Draft: 18/04/13



IMPACT ASSESSMENT CHECKLIST – CCTV IN …….

Impact Assessment	Response
What organisation will be using the CCTV images?	
Who will take legal responsibility under the Data Protection Act (DPA)?	
What is the organisation's purpose for using CCTV? What are the problems it is meant to address?	
What are the benefits to be gained from its use?	
Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?	
Do we need images of identifiable individuals, or could we use other images not capable of identifying the individual?	
Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?	
What future demands may arise for wider use of images and how will we address these?	
What are the views of those who will be under surveillance?	
What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?	

APPENDIX 6

CONFIDENTIALITY (NON-DISCLOSURE) AGREEMENT

Confidentiality Agreement between the Kingdom Housing Group (Kingdom).

and

…….. (you)

You shall have access to confidential information of Kingdom and you agree to:

(1) keep all information (whether written or oral) confidential concerning the business, tenants, staff and clients of the Kingdom that it may obtain or receive as a result of the work carried out by you for Kingdom ("Confidential Information")

(2) not disclose any Confidential Information without the consent of Kingdom to any other person other than its staff involved in the services to be provided.

(3) only allow staff of the company who have a need to know the information and to use the Confidential Information solely in connection with the implementation and performance of the services and not for its own benefit or for the benefit of any third party. In particular the Company is hereby prohibited from:
- publishing, transmitting or otherwise disclosing or allowing access to any of the Confidential Information to any third party in any way;
- using any of the Confidential Information for any purpose other than for the performance of the services;
- copying or reproducing any of the Confidential Information in any manner or form or the storing of any confidential information in any electronic, digital or other form or medium and allowing access by any other party or using the Confidential Information or any part of it in any manner which is prejudicial to the interests of Kingdom;

(4) The Company shall retain such Confidential Information (where permitted) by storing it in safe-keeping under secure conditions in a place not generally accessible to unauthorised parties. The Company will immediately upon request undertake to return to Kingdom all confidential information in whatever form together with any and all copies in their possession and control.

(5) In the event of the Company breaching any of the conditions in this agreement or if Kingdom has reasonable grounds for believing that such a breach either has occurred or will occur, Kingdom will be entitled to instruct the immediate cessation of use by the Company or any other third party of all confidential information and the return of the confidential information.

(6) The Company undertakes to indemnify and keep Kingdom fully and effectively indemnified against all actions, costs, losses, claims, damages and expenses of any kind or nature arising from any breach or non-performance of any of the representations, undertakings or obligations contained within this agreement.

Signed: ……... Date: ……

KINGDOM HOUSING GROUP

DATA PROTECTION POLICY

Policy drawn up with reference to:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx
Information Commissioner's CCTV Code of Practice (Revised Edition 2008)
Law at Work Sample Data Protection Policy
Information Commissioner's Office – Data Protection Good Practice Note
SFHA – Raising Standards in Housing – Access to Information
EVH – Data Protection Information Note

Reference made to the following sources and other guidance:

Cross Reference to Performance Standards for social landlords and homelessness functions: Guiding Standards: GS3.5.

Reference to the current Data Protection Policy which has been operational since December 2002.

Prepared by: Lesley Proudfoot, Resources Services Co-ordinator

Draft 1: Data Protection Reps on 6 March 2013
Draft 2: Joint Directors/Managers Review on 3 May 2013
Draft 3: audited by (Legal) on 10 June 2013
Draft 4: circulated to the JCG on 19 July 2013 last date for comment 16 August 2013

Sub Committee Review of Policy on 26 November 2013

Presented for discussion and to Committee of Management on 16 December 2013
Policy Approved Yes

To be Presented for discussion and to Board of Directors on 14 March 2014
Policy Approved Yes / No

Next review date: No later than December 2018