

NEXT STEP HOMES LIMITED

DATA PROTECTION POLICY

1. Policy Statement

Next Step Homes Limited is registered in terms of the Data Protection Act 1998 and is totally committed to the principles of that Act. Those principles are reproduced as an appendix to this Policy Statement.

The Association will look to its managing agent, Langstane Housing Association Limited, to discharge all of its duties and responsibilities under the Act other than those which are the direct responsibility of this Association. The managing agent will put in place procedures for ensuring that all data held is held and processed in accordance with the Act and that all persons with a legitimate interest in the data can access that information within a reasonable timescale, in an intelligible form, and at reasonable costs. The managing agent will also introduce a comprehensive set of security measures to ensure that relevant data is held and processed only by relevant staff and that no unauthorised access can be obtained.

2. Data Controller

The Chief Executive of the managing agent is the Association's Data Controller in terms of the Act. It is his responsibility to ensure that the terms of the Act, the 8 principles, and the requirements of this Policy are fully complied with.

3. Departmental Liaison Officers

Within each of the managing agents' departments of Customer Services, Corporate Services and Business Development there are appointed persons who act as Departmental Liaison Officers. Their functions are to review the data held within the department, to advise the Data Controller of the information and data held both manually and electronically within the department, to identify such data as may no longer be appropriate to be retained and to ensure its safe and confidential disposal. They should also act as informal advisers to staff within their respective departments on the implications of the Act and this Policy. Under the direction of the Data Controller they should also review the security of the data held to ensure that only authorised persons have access.

4. Data Protection Working Party

The Data Controller and the appointed Departmental Liaison Officers shall collectively form the Data Protection Working Party. This Working Party shall be chaired by the Data Controller, meet from time to time to review the operation of this Policy and to discuss other matters relating to the holding, processing and accessing of data.

5. Rights of Access

The Association recognises the legitimate rights of individuals, to be aware of and where appropriate have access to relevant data held concerning them, subject to the rights of third parties. Persons who wish to obtain access to relevant data held concerning them should make application to the Data Controller in writing, specifying as far as possible the range and type of information sought.

The managing agent, on behalf of the Association, undertakes, subject to the payment of the appropriate fee and the receipt of a proper request, to issue relevant data held about individuals to that individual within 20 working days. The fee for each individual request will be determined by the Data Controller but should be subject to a maximum of £20 (Twenty Pounds) for one request.

6. Training

As part of its responsibilities, the managing agent undertakes to provide a comprehensive training plan to ensure that everyone concerned understands the implications of the Act and the scope of this Policy and in particular understands the responsibilities placed on them in the processing of data.

7. Policy Review

This Policy will be formally reviewed and, if felt appropriate, amended at intervals of not less than 2 years.

Date Approved by Committee of Management: 03.02.10
(Approved as interim policy for one year pending group structure)

Review Period: 1 Year

Date Due for Review: February 2011

DATA PROTECTION POLICY - PRINCIPLES

The processing, retention and control of data in terms of the Data Protection Act 1998 are all subject to 8 principles set out in Part 1 of Schedule 1 to the 1998 Act. The following is a list of the 8 principles.

1. First Principle

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless one of the conditions below is met and in the case of sensitive personal data, where the data subject has given explicit consent and the processing is necessary”.

2. Second principle

“Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes”.

3. Third Principle

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.

4. Fourth Principle

“Personal data shall be accurate and, where necessary, kept up to date”.

5. Fifth Principle

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

6. Sixth Principle

“Personal data shall be processed in accordance with the rights of data subjects under this Act”.

7. Seventh Principle

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, “personal data”.

8. Eighth Principle

“Personal data shall not be transferred to any country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data”.