Policy title:	Data Protection Policy		
Scope:	Group-wide		
Policy owner & job title:	Paul Medford, Group Company Secretary		
Approver:	Group Audit & Risk Committee		
Date:	11/01/2017	**Review Due Date:**	31/12/2018

POLICY SUMMARY:

- The Data Protection Policy covers the use of personal data by all colleagues across Aspire Housing (including volunteers, work placements, students etc.), as well as that accessed and handled by any contractors, suppliers and agencies working on the Group's behalf.
- Personal data may belong to customers, colleagues or any other individual that has dealings with the Group.
- Colleagues are required to adhere to the 8 principles of the Data Protection Act 1998 as described in the policy.

ASSOCIATED POLICIES AND PROCEDURES:

- Aspire Housing Document Retention Policy
- Aspire Housing Code of Conduct and Probity Policy
- Aspire Housing Information Security and Systems Usage Policy

1. POLICY STATEMENT

a. Introduction

The purpose of this document is to provide guidance for staff in order to meet the requirements of The Data Protection (DPA) Act 1998.

The Data Protection Act 1998 received the Royal Assent on 16th July 1998 and came into force on 1 March 2000, replacing the Data Protection Act 1984. It deals with the use of data and its purpose is to protect information about individuals and to enforce a set of standards for the processing and use of such information.

This policy applies to Aspire Housing. For the purposes of this policy, Aspire Housing is defined as Aspire Housing, PM Training, the Realise Foundation and any future entrants to the Group.

b. Scope

This policy applies to all electronically held data (on computers, ipads, mobile phones, hand held personal digital assistants (PDA), mobile data storage, e.g data/memory sticks, and scanning and duplication equipment) used by, or on behalf of Aspire Housing, regardless of location and to all paper files held (including manual filing systems and card indexes). It also relates to information held or accessed via colleagues' own personal devices, in so far as that information relates to Aspire Housing.

This policy also relates to personal data held in connection with CCTV footage and call recordings across the Group. Aspire Housing uses close circuit cameras on its premises for the purpose of security and safety.

The Construction Industry Training Board (CITB) requires PM Training to store CCTV of learner registration and testing, and may request to view CCTV footage for a period of up to 30 days after CCTV has been collected. The PM Training Administrator/ Receptionist will have accessibility to the CCTV footage and will be responsible for authorising requests for CCTV footage from the CITB.

Data protection is a group wide responsibility and co-operation to ensure that Aspire Housing complies with the legal requirements of The Data Protection Act 1998 and any subsequent legislation is essential.

The obligations contained in this policy apply to all those who have permission to access data held by Aspire Housing. This includes all colleagues in Aspire Housing (including volunteers, work placements, students etc.), as well as any contractors, suppliers and agencies who have access to and handle personal data, while carrying out work on Aspire Housing's behalf.

c. Equality & Diversity Impact Assessment

This policy has been considered against our Equality and Diversity Policy and no additional provisions are required.

It is noted that Aspire Housing collects and processes a range of personal and sensitive data about its customers. This allows for a better understanding of customer needs and supports the delivery of an excellent service regardless of age, disability, ethnicity, faith, gender or sexuality. It is imperative that we meet the requirements of the Data Protection Act when collecting or processing customer data.

d. Objectives:

- To set out the principles of Aspire Housing's approach to data privacy & protection;
- To provide guidance on the principles and definitions of the Data Protection Act 1998.

2. POLICY OVERVIEW

Aspire Housing regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining customer and colleague confidence, as well as that of prospective employees and learners. We ensure that our organisation treats personal information lawfully and correctly.

To this end we fully endorse and adhere to the Principles of data protection, as detailed in the Data Protection Act 1998.

There are currently no companies within the Group subject to the Freedom of Information Act 2000, except in relation to any contracts we are delivering on behalf of public authorities that are subject to the Act (as listed in Schedule 1 to the Act).

3. RESPONSIBILITY

Compliance with the Act is the responsibility of everyone within Aspire Housing, whether as individual collectors, keepers or users of personal data. Therefore colleagues are required to be aware of the provisions of the Data Protection Act 1998, such as keeping records up to date and

accurate, and its impact on the work they undertake on behalf of Aspire. It is the responsibility of managers to monitor compliance with the policy, particularly in respect of data retention.

It is **not** the responsibility of the Data Protection Officer to apply the provisions of the Data Protection Act.

Detailed responsibilities are set out in the Data Protection Manual. See also items 7 & 8.

4. DATA PROTECTION DEFINITIONS AND PRINCIPLES

a. Key Definitions

Personal data means data which relates to living individuals who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. It also 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 relating to the data subject which includes information such as: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexuality; information relating to commission of criminal offences.

Processing means obtaining, recording or holding information or data or carrying out any operation or set of operations on that data.

Data subject means an individual who is the subject of personal data.

Data controller means a company or person who determines the purposes for which, and the manner in which personal data is processed. In this context this relates to Aspire Housing as an organisation.

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.

b. Data Protection Principles

The Act contains eight principles for the processing, management and security of personal data and if these principles are not adhered to or our arrangements for compliance prove to be inadequate then Aspire may be liable for damages for any loss/harm caused to individuals, possibly resulting in a fine of up to £500,000. It is therefore essential that the measures we establish for compliance with the requirements of the Act are robust, implemented consistently and maintained.

(1) Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

a) at least one of the conditions in Schedule 2 is met; and

b) in the case of Sensitive Personal Data, at least one of the conditions in Schedule 3 is **also** met.

See Appendices 1 and 2 for detail.

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

(4) Personal data shall be accurate and, where necessary, kept up to date.

(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

(7) 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) Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

5. MONITORING

The Data Protection Policy and accompanying procedures will be reviewed by the Group Company Secretary every two years. The review will ensure that the policy and procedures comply with all current legislation, regulatory guidance and recommended good practice.

6. GUIDANCE

Further details and written guidance regarding compliance with the Act is contained in the Data Protection Manual.

If you have any queries about any aspect of this document or of Data Protection legislation please contact the officer mentioned below:

Paul Medford – Data Protection Officer

7. RESPONSIBILITIES OF EMPLOYEE

All Group employees are required to be aware of the provisions of the Act, such as keeping records up to date and accurate, and its impact on the work they do.

Any breaches of this policy and the supporting Data Protection Manual, whether deliberate, or through negligence, may be considered a breach of the Group's Probity Policy and may result in disciplinary action being taken, which may include dismissal, or even a criminal prosecution.

8. RESPONSIBILITY OF ASPIRE HOUSING

Aspire Housing is required to comply with the legal requirements of the Data Protection Act 1998 and any subsequent legislation or regulations.

Appendix 1 : Schedule 2, Data Protection Act 1998
Conditions relevant for the processing of any personal data.

1. The data subject has given his consent to the processing.

2. The processing is necessary—

   (a) for the performance of a contract to which the data subject is a party, or

   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary—

   (a) for the administration of justice,

   (b) for the exercise of any functions conferred on any person by or under any enactment,

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

   (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix 2 : Schedule 3, Data Protection Act 1998
Conditions relevant for the processing of sensitive personal data.

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

   (2) The Secretary of State may by order—

   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—

   (a) in order to protect the vital interests of the data subject or another person, in a case where:

      (i) consent cannot be given by or on behalf of the data subject, or

      (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—

   (a) is carried out in the course of its legitimate activities by any body or association which—

      (i) is not established or conducted for profit, and

      (ii) exists for political, philosophical, religious or trade-union purposes,

   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

   (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—

   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

   (b) is necessary for the purpose of obtaining legal advice, or

   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary—

      (a) for the administration of justice,

      (b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

[7.A. (1) The processing –

(a) is either –

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any incorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.]

8. (1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.