Policy title:	Data Protection Policy		
Scope:	Group-wide		
Policy owner & job title:	Head of Governance		
Approver:	Audit Committee (Minutes with approval available on request)		
Date:	1/6/2020	**Review Due Date:**	1/6/2022

POLICY SUMMARY:

- The Data Protection Policy covers the processing of personal data across Aspire Housing, its associated companies processed and data processors working on the group's behalf.
- Personal data may belong to customers, learners, colleagues or any other individual that has dealings with the group.
- Colleagues are required to adhere to the data protection principles set out in article 5 of the General Data Protection Regulations (GDPR). They should also respect the rights individuals have under the GDPR.

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
- The Data Protection Manual
- Personal Data Breach Procedure
- Privacy notice and forms guidance
- Enforcing Individual Rights Procedure
- Data Protection Impact Assessment Procedure

1. POLICY STATEMENT

Introduction

This policy applies to the group. For the purposes of this policy, the group is defined as Aspire Housing, Achieve Training, the Realise Foundation and any future entrants to the group.
The purpose of this document is to layout and provide guidance on how the group meets the requirements of the General Data Protection Regulation (GDPR), and the Data Protection Act (DPA) 2018

Scope

Article 9(2)(b) of the GDPR states that all data controllers should have an appropriate Data Protection Policy in place.
Aspire Housing, Achieve Training and the Realise Foundation are each registered as a Data Controller with The Information Commissioners Office (ICO). Aspire Housing also acts as a

Data Processor for Achieve Training and the Realise Foundation under a written Service Level Agreement (SLA) for the provision of IT, HR, Facilities management and other corporate services.

This policy demonstrates how the group complies with the principles and responsibilities of accountability set out in Article 5(2) of the GDPR.

This policy applies to all electronically held personal 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 the group , 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 the group.

This policy also relates to personal data held as CCTV footage and call recordings across the group.

The obligations contained in this policy apply to all those who have permission to access data held by the group. This includes all colleagues in the group (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 the group's behalf.

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 the group collects and processes a range of personal and sensitive data about its customers/ learners, allowing for a better understanding of their needs and the delivery of an excellent service. It is imperative that we meet the requirements GDPR when collecting or processing personal data.

2. POLICY OVERVIEW

The group regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining confidence. To ensure that our organisation treats personal information lawfully and correctly we fully endorse the principles of data protection, as detailed in the GDPR.

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.

3. DATA PROTECTION DEFINITIONS AND PRINCIPLES

Key Definitions

Data controller means a company or person who determines the purposes for which, and the manner in which personal data is processed.

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

Data processor, in relation to personal data, means any organization who processes the data on behalf of the data controller.

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.

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

Sensitive personal data (also referred to as "special categories of personal data" under GDPR) means personal data relating to the data subject which includes information such as: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

Data Protection Principles

Article 5 of the GDPR specifies a number of principles for the processing, management and security of personal data. If these principles are not adhered to or our arrangements for compliance prove to be inadequate, the Data Controller may be liable for a fine from the Information Commissioners Office of up to €20 million or 4% of annual turnover. It is therefore essential that the measures established for compliance with the requirements of GDPR are robust, implemented consistently and maintained.

Below we have detailed the principle in Article 5 of the GDPR that all staff should abide by.

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(See Appendix 1 and 2 - In order to process personal data you must identify a lawful basis at Article 6. In order to lawfully process sensitive personal data (also known as special category data), you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. The lawful basis for processing must also be stored in our register of personal data).

b) 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 not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

Criminal offence data

To process personal data relating to criminal convictions and offences we must have a lawful basis for processing under Article 6 (see appendix 1), in exactly the same way as for any other personal data. However, we must also process in compliance with schedule 1 part 3 of the Data Protection Act 2018 (see appendix 3).

Accountability and Governance

The accountability principle in Article 5(2) requires organisations to demonstrate that they comply with the principles of accountability. Aspire Housing are expected to put into place comprehensive but proportionate governance measures to minimise the risk of breaches and uphold the protection of personal data.

Data Protection officer (DPO)

The group have chosen to appoint a DPO as per section 4 of the GDPR. The DPO's role is to assist with the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs), and act as a contact point for data subjects and the supervisory authority.

The DPO will have a relevant qualification in Data Protection, and to ensure independence will be a member of the Governance team. Ordinarily the DPO will report into the Company Secretary, but where necessary the DPO may report directly to any Executive Director or the Chair of the Audit Committee

The DPO shall have the authority, autonomy and decision-making powers to manage noncompliance and breaches, including reporting such incidents to the relevant supervisory authority.

The DPO has to strike a balance between being a trusted advisor and the internal policing

role. The nature of the role has a level of independence, due to protected mechanisms within the GDPR:

- The DPO shall have all necessary co-operation and access to systems holding personal data for the execution of their task. (Article 38.2)
- The DPO shall not receive any instructions from the Data Controller or Processor regarding the exercise of any DP task. (Article 38.3)
- Data subjects (customers/ learners or employees) will be able to contact the DPO regarding all
  issues relating to processing of their personal data. (Article 38.4)
- The DPO shall be bound by secrecy or confidentially regarding the performance of their tasks. (Article 38.5)

Staff Training and awareness

Aspire Housing ensures that new members of staff complete data protection training as part of their induction. Role-based training modules are also available for certain roles and must be completed where appropriate. All staff should complete data protection training within two years of their last training. Records of staff training will be kept by HR and they will coordinate any refresher training. If a data breach or near miss would occur, then the member of staff may be required to carry out further training and there would be communications to all staff.

All staff have access to a data protection page on the intranet which includes a Data Protection Manual and other useful information to ensure staff comply with data protection.

Internal audits and Internal control

To ensure that each service area is working in compliance with the GDPR the DPO will assist with and conduct data protection audits.

There is also an annual internal control checklist that is distributed to heads of service to ensure compliance with this policy and associated procedures. This can be found in the data protection manual.

Key performance indicators have been created to assess the effectiveness of how the organisation deals with data protection.

Privacy by design

Under the GDPR Aspire Housing has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data as in Article 5 (above) and also ensuring that the minimum personal data (data minimization) is used to carry out activities (Article 23).

Aspire Housing has developed a Data Protection Impact Assessment (DPIA) framework that should be completed for all new projects or where processing activities have been subject to change. Please see the DPIA template and guidance.

Data Retention

Article 5(1e) of the GDPR specifies that personal data should not be kept longer than required. Aspire Housing has a document retention policy that specifies when documents should be destroyed. This is being reviewed in line with GDPR compliance to go beyond documents and look at all types of personal data held. The organisation is in the process of identifying how data can be deleted from systems and has a process for upholding individual rights.

Data Security

Article 5(1f) specifies that organisations should have appropriate measures of security in place to protect personal data. All employees must ensure that all personal data they hold is kept securely and is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Data Security should be undertaken in line with the Information Security and Systems Usage Policy, which sets out the responsibilities of the employee and the Aspire Housing. The Data Protection Manual also provides detailed information on data security procedures.

Aspire Housing have been certified to be compliant with the requirements of the Cyber Essentials Scheme. Aspire Housing have documented a description of the technical and organisational security measures in place to satisfy Article 30 of GDPR, which for security purposes can be found in a separate document. This description has been taken from the Cyber Essentials Standard.

To monitor IT security penetration testing is carried out annually by an external organisation.

To monitor physical security of premises the group uses closed circuit cameras on its premises. At Kingsley, the largest of the premises; there is a system of ID cards to identify individuals and gain entry to premises. ID cards are required to be worn by staff at all times and access may be limited to the needs. In other premises the only entrance to buildings is through a reception area where visitors can be challenged as to their legitimacy and must sign in to gain entry to the building.

The group promotes a culture of clear desks and workspaces.

International transfers

It may sometimes be necessary for the group to transfer personal information overseas. If the transfer involves the data leaving the EU the group will ensure the requirements of GDPR Chapter 5 are met.

Data Protection Registers

To satisfy Article 30 of the GDPR Aspire Housing keep a Register of Processing Activities (RoPA) which includes a description of the data, the purpose, where the data is stored, who uses the data, relevant legal grounds from Article 6 and Article 9 (see appendix 1 and 2), who it may be shared with, and if it contains data about children. If the group wishes to change the way personal data is processed or process new types of personal data then they should inform the DPO and amend the RoPA.

The group have also classified suppliers and contractors within the contracts register into whether they are data processors and data controllers.

Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Article 33 of the GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. All organisations must do this within 72 hours of becoming aware of the data breach, where feasible.

Aspire Housing have a Personal Data Breach procedure that outlines the process in the event of a data breach. A record is kept of all data breaches and near misses.

If a member of staff becomes aware of a data breach then they should report it to the DPO immediately.

Third party suppliers and contractors

Whenever a data controller uses a data processor (a third party who processes personal data on behalf of the controller) they need to have a written agreement in place. Similarly, this also applies if a data processor employs another data processor. The agreement must include certain specific terms.

The group have standard GDPR contractual clauses that should be added to data processor contracts. For all data controllers a data sharing agreement should be in place. All staff should ensure that they are compliant with GDPR when dealing with 3rd parties. The data protection manual contains further guidance on this and the standard clauses can be found in its appendices.

Personal data of children

Under GDPR the legal age of a child is 18 years old. Where we are collecting personal data of children under the age of 13 based on the lawful ground of consent at Article 6 (see appendix 1 and 2), we will need to have the consent of the parent or guardian to process that personal data. If a child is age 13 or over then the child will be considered old enough understand consent, and we can lawfully obtain consent from that child.

The group verify the ages of all staff, tenants and learners when they apply for the service by asking to see identification to prove age. If Aspire Housing are informed of an additional occupant of a tenancy then they are also required to prove age with identification. This allows the organisation to understand the ages of individuals so that Aspire Housing can comply with the regulation around children.

Consent

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It also requires individual ('granular') consent options for

distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. The privacy notice and forms guidance set out how consent should be obtained to the standard of GDPR when we obtain personal data and process it based on consent.

The GDPR gives a specific right to withdraw consent. We need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time. The group have an individual rights procedure that details how we enable the right to object. Users of the customer portal have the ability to amend their consent options within the portal.

Individuals rights

Aspire Housing respects the rights that individuals have over their personal data and have procedures in place to enforce these rights (please see the individual rights procedure). The individual rights under GDPR are as follows:

- The right to be informed (Articles 13 and 14)
- The right of access (Article 15)
- The right to rectification (Articles 16 and 19)
- The right to erasure (Articles 17 and 19)
- The right to restrict processing (Articles 18 and 19)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 22)

The Data Controllers within the group have privacy notices on their websites detailing all of the types of processing that is carried out in relation to Article 13. There is also a procedure giving guidance on the writing of privacy notices and the collection of personal data in forms. All staff should follow the guidance when collecting personal information from individuals.

Article 15 of the GDPR gives individuals the right to access their personal data and other supplementary information to allow them to verify the lawfulness of the processing. This is often referred to as a subject access request (SAR). Aspire Housing have a procedure for complying with SARs. All SARs should be dealt with free of charge and within one month of their receipt. For this reason it is essential that staff recognise a SAR when it is received and inform the DPO who will provide guidance on how the SAR will be undertaken.

The group have a procedure for complying with the right to rectification. Where possible staff will aim to carry out the rectification straight away, however if a member of staff is unsure about carrying out the rectification of personal data, the amendment is complex, or it is believed to be unfounded then they should contact the DPO.

For the right to rectification, erasure, restriction of processing, data portability, the right to object, and rights in relation to automated decision making and profiling the group has a procedure to review each case for eligibility and then action requests with the help of IT and other departments. Staff should be aware that none of these rights are absolute and the procedure covers the eligibility in detail.

4. MONITORING

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

5. GUIDANCE

Further details and written guidance regarding compliance with the GDPR 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 Data Protection Officer by email; DPO@aspirehousing.co.uk

The Information Commissioners Website is also a good resource for data protection information:

https://ico.org.uk

6. RESPONSIBILITIES OF EMPLOYEE

Compliance with this policy, GDPR and the DPA 2018 is the responsibility of everyone within the group. Colleagues are required to be aware of this policy and the provisions of data protection law and its impact on the work they undertake on behalf of the group. It is the responsibility of managers to monitor compliance with the policy, particularly in respect of data retention. Detailed responsibilities are set out in the Data Protection Manual.

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.

It is also worth noting that section 198 of the DPA 2018 provides that where a company commits an offence under GDPR, and it is proven that it was done with the consent, connivance or with attribution to the negligence of a director or officer, then the director or officer will be guilty of the offence as well as the company. If guilty of an offence an individual may be personally liable for a fine.

7. RESPONSIBILITY OF THE GROUP

The group is required to comply with the legal requirements of the GDPR and any subsequent legislation or regulations.

Appendix 1 – Article 6 - Lawfulness of processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 2 – Article 9 - Special Categories of Data

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular

contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 3 – The Data Protection Bill - Schedule 1, Part 3 conditions – processing criminal convictions data

- **Consent** - Processing with the consent of the data subject.
- **Protecting individual's vital interests** - Processing of criminal convictions data necessary in the vital interests of an individual.
- **Processing by not-for-profit bodies** - Processing in the course of legitimate activities pursued by a not-for-profit body with a political, philosophical, religious or trade union aim where the processing relates to members, former members or persons with regular contact with the body.
- **Personal data in the public domain** - Processing where personal data is manifestly made public by a data subject.
- **Legal claims** - Processing is necessary for purpose of: (i) any legal proceedings; (ii) obtaining legal advice; or (iii) establishing, exercising or defending legal rights.

- **Judicial acts** - Processing is necessary when a court or tribunal is acting in its judicial capacity.
- **Administration of accounts used in commission of indecency offences involving children -** Processing for certain indecency offences processing involving children necessary for administering an account relating to the payment card used in the commission of the offence or cancelling the card used. In order to meet this condition, the controller must have an appropriate policy document in place, as required under Part 4 of Schedule 1
- **Extension of certain conditions under Schedule 1, Part 2** - Allows processing of criminal convictions data, where processing would meet a condition in Schedule 1, Part 2 except for the fact it must satisfy the substantial public interest test, provided the controller has an appropriate policy document in place and meets the additional safeguards in Part 4.
- **Extension of insurance conditions** - Should the processing of personal data not reveal racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, then this extension allows processing where it would otherwise meet the insurance condition in Schedule 1, Part 2, or the condition relating to the extension of certain conditions under Schedule 1, Part 2 stated above (when processing criminal convictions data).

Appendix 4 – Notes

The Construction Industry Training Board (CITB) requires Achieve 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 Achieve Training Administrator/ Receptionist will have accessibility to the CCTV footage and will be responsible for authorising requests for CCTV footage from the CITB.