Policy title:	Data Protection Policy		
Scope:	Group-wide		
Policy owner & job title:	Company Secretary		
Approver:	Audit and Risk Committee		
Date:	July 2024	**Review Due Date:**	July 2026

POLICY SUMMARY:

- The Data Protection Policy covers the processing of personal data across the Aspire group (Aspire Housing and its subsidiaries) and data processors working on the group's behalf.
- Personal data may belong to customers, colleagues or any other individual that has dealings with the group.

ASSOCIATED POLICIES AND PROCEDURES:

- Aspire Housing Data Retention Policy
- Aspire Housing Code of Conduct and Probity Policy
- Aspire Housing Information Security and Systems Usage Policy
- UK GDPR - Data Protection Manual
- Personal Data Breach Procedure
- Data Subject Access Request Procedure
- UK GDPR - Individual Rights Procedure
- Privacy Notice Guidance Procedure
- Data Protection Impact Assessment Procedure
- CCTV Policy and Procedure
- Appropriate Policy Document

1. POLICY STATEMENT

Introduction

The purpose of this document is to layout and provide guidance on how the group meets the requirements of the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act (DPA) 2018

This policy applies to the Aspire group. For the purposes of this policy, the group is defined as Aspire Housing, Incana Sales, Durata Development and any future entrants to the group.
Aspire Housing is registered as a Data Controller with The Information Commissioners Office (ICO). Aspire Housing also acts as a Data Processor for Incana Sales and Durata Development under a written Service Level Agreement (SLA) for the provision of IT, HR, Facilities management and other corporate services.

Scope

Aspire Housing complies with data protection legislation guided by the six data protection principles.

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- adequate, relevant and limited to what is necessary.
- accurate and, where necessary, kept up to date.
- kept in a form which permits identification of data subjects for no longer than is necessary.
- processed in a manner that ensures appropriate security.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to regulatory fines or claims for damages from data subjects. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

Equality & Diversity Impact Assessment

This policy has been considered against our Equality and Diversity Policy with an Equality and Diversity Impact Assessment completed (EDIA). , Based on recommendations arising from the EDIA it is noted that:-

- Where customers have specific needs to access the policy, reasonable support would be given. By way of example, this may include the provision of the policy in alternate forms such as braille, large print or audio versions and ensuring that the processes followed within the policy are reasonably adapted to reflect the needs of the individual.
- The Data Protection Officer will be happy to provide advice on specific matters related to protected characteristics as defined under the Equality Act 2010 where needed.

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

2. POLICY

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life and/or sexual orientation
- Criminal data (convictions and offences)

Information Asset Owners – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid Aspire in managing personal data and its associated risks.

Privacy Notices - we publish a privacy notice on our websites and provide timely notices where this is required. New customers are provided with a link to the privacy notice when then start their tenancy. We also publish an employee privacy notice which is shared with colleagues when they join and kept up to date.

Colleague Training and Awareness

Aspire Housing ensures that new colleagues 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 colleagues should complete data protection training within two years of their last training. Records of colleague training will be kept by HR, and they will coordinate any refresher training. If a data breach or near miss occurs, then the colleague may be required to carry out further training and there may be communications to all staff around the breach/near miss for awareness/training purposes.

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

Data Protection by Design and Default

Under the UK 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 minimisation) 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.

Data Protection Registers

To satisfy Article 30 of the UK GDPR, the group maintains a Register of Processing Activities (RoPA). If the group wishes to change the way that personal data is processed or process new types of personal data then they should inform the DPO and the relevant Head of Service should amend the RoPA.

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 UK 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.

The group has a Personal Data Breach procedure which 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 has standard UK GDPR contractual clauses that are added to data processor contracts. For all agreements where Aspire and a third party are jointly acting as data controllers a data sharing agreement should be in place. All staff should ensure that they are compliant with UK 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.

Individual Rights

We have clear processes to handle subject access requests and other information rights requests under the responsibility of the Data Protection Officer.

Policies and Procedures
We produce policies and guidance on information management and compliance that we communicate to staff.

Communications
We clearly communicate and seek to embed a culture of privacy and risk orientation.

3. 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.

4. GUIDANCE

Further details and written guidance regarding compliance with the UK GDPR is contained in the GDPR - 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

5. ROLES AND RESPONSIBILITIES
RESPONSIBILITY OF THE GROUP

The group is required to comply with the legal requirements of the UK GDPR, Data Protection Act 2018 and any subsequent legislation or re**DATA PROTECTION OFFICER**
The group has an appointed person to have oversight of compliance with Data Protection legislation. Their 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 appointed person shall have the authority, autonomy and decision-making powers to manage non-compliance and breaches, including reporting such incidents to the relevant supervisory
authority.

DATA AND SECURITY OVERSIGHT (DASO) GROUP

DASO is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Executive Team on information governance with data protection and compliance decisions.

INFORMATION ASSET OWNERS (IAO)

IAOs have local responsibility for data protection compliance in their area/directorate.

EMPLOYEES

Compliance with this policy, UK 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 UK 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.