THE HAVEBURY HOUSING PARTNERSHIP

DATA PROTECTION POLICY (GP 016)

Unique Reference No	**GP016**
Date created	17 January 2023
Date for review	January 2025
Author	Assistant Director of ICT
Version Number	4
Status	Board Approved (28 February 2023)
Accountable Director	Director of Resources and Company Secretary
Equality & Diversity Impact Assessment	Low

1. Responsibility

The Board has overall responsibility for compliance with data protection legislation and this Policy. The Assistant Director of ICT will provide operational support for data protection and will act as liaison with the Data Protection Officer.

All employees and members, agency workers, appointed agents and contractors are responsible for data protection and complying with the law and are obliged to follow this Policy, report any breaches of this Policy and attend any training required.

2. Definitions

Anonymisation – keeping a record but clearing the personal data.

Breach – an incident which has highlighted non-compliance with the General Data Protection Regulation.

Data Controller – an organisation, such as Havebury Housing Partnership, that controls the flow of personal data collected by it about Data Subjects.

Data Processor – an organisation working under contract with a Data Controller on their behalf that processes personal data.

Data Processing Agreement – Data Processors must only act on the written instructions of the Data Controller. Standard clauses are part of the contract between the Data Controller and the Data Processor.

Data Protection Officer – an independent expert in data protection whose role is to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding the impact of processing personal data and act as a contact point for data subjects and the Information Commissioner.

Data Sharing Protocol – an agreement for the sharing of personal data amongst Data Controllers (as opposed to Data Processors, an example being where we share data legally with Local Authorities or Police).

Data Subject – an individual whose personal data is being processed.

DPIA – Data Protection Impact Assessment, used to identify privacy or DP concerns before implementing new way of processing personal data.

Near-breach - an incident where a breach would have occurred except for an unexpected action or set of circumstances which prevented it

Personal data – as defined in Article 4 of GDPR means any information relating to a person, identified or identifiable from that data either directly or indirectly, in an electronic or paper structured filing system.

Pseudonymisation – replacing personal data with an identifier that cannot be used to identify the Data Subject except from a separate limited-access set of records.

Special category data – this is personal data that needs more protection because it is sensitive – it is prescribed as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, a person's sex life; or a person's sexual orientation. We also consider criminal convictions and offences data to be special category data.

Sub-processor – an organisation which processes data on behalf of a Data Processor with whom we have shared personal data.

3. Aims and Objectives

3.1 This policy reflects our commitment to respecting the rights and privacy of individuals.

3.2 To ensure that personal data is processed in a manner compliant with legislation and to appropriately manage risks associated with the processing of personal data

3.3 To establish an open and transparent environment in which Data Subjects are in control of their personal data and are fully informed of their rights and the legal basis for which their data may be used.

4. Policy Statement

4.1 This Policy applies to all personal data that we process on behalf of Data Subjects for whom Havebury acts as Data Controller or Data Processor and their personal data.

During all decision making on processing personal data, we will uphold the principles laid down in Article 5 of UK GDPR:

- We will only process personal data lawfully and fairly.
- We will declare to Data Subjects the purpose for which it is processed.
- We will only use it for the purpose declared.
- We will only process the minimum amount of personal data for the purpose.
- We will ensure that data is accurate.
- We will only keep it for as long as necessary for the purpose.
- All personal data will be kept secure and treated as confidential.
- As a Data Controller, we will demonstrate compliance with the six principles above.

4.2 There must be a legal basis for all personal data processed as defined in Article 6 of UK GDPR. In the case of Special Category Data, there must be an additional legal basis from Article 9 of UK GDPR . At the point of collecting personal data, this legal basis will be explained to the Data Subject and they will be notified about their rights and given details about how their data will be used. Where personal data is provided by a third-party, the Data Subject will be informed as legally required.

We will process criminal convictions and offences data as Special Category Data. The legal basis will be from the applicable grounds in Schedule 1 of the Data Protection Act 2018.

4.3 If the legal basis is Consent from the Data Subject, this must be informed, freely-given, specific and unambiguously collected. It may be withdrawn at any time and a clear set of procedures will be available for Data Subjects to exercise this right. Data Subjects under 13 years of age will require Consent from a parent or guardian.

If the legal basis for processing is legitimate interest of the Data Controller, a Legitimate Interest Assessment will be undertaken.

4.4 In addition to the legal basis for personal data processing, we will maintain a data retention schedule and procedures for erasure, destruction, anonymisation and pseudonymisation of personal data. Personal data will be processed in accordance with the legal basis as explained to the Data Subject and they will be reminded to inform of us of changes to their personal data. For paper documents containing personal data, this must be subject to destruction through our corporate shredding facilities.

4.5 We will respect the rights of Data Subjects including:

- the right to be forgotten;
- the right to object to processing;
- the right of data portability;
- the right of access;
- the right of rectification if data is incorrect;
- the right to be informed; and
- the right to restrict processing.

A clear set of procedures will be available for Data Subjects to exercise these rights.

If we carry out profiling and/or automated decision-making, we will ensure that in addition to the principles in paragraph 4.1, above, that:

- we have also additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups including children;
- we carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling;

- we tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from; and
- we will use anonymised data in our profiling activities.

4.6 We uphold the principles of data protection by design and default. Any new processing activities or technology changes involving personal data will be subject to a screening process that establishes whether a Data Protection Impact Assessment (DPIA) is required prior to the new or changed activity being implemented. A DPIA will always be undertaken and approved by the Data Protection Officer where there is a high risk to the rights and freedoms of data subjects, and any risks managed accordingly. We will document the outcome of DPIAs to demonstrate legal and regulatory compliance.

4.7 We are accountable as the Data Controller and we ensure that those Data Processors working on our behalf are managed appropriately.

We will include a compliance clause in all contracts with Data Processors to enforce our control over the use of sub-processors and we will, at our discretion, assess the risk presented by a Data Processor at the procurement selection stage and then annually for the length of the contract. A Data Processing Agreement will be in place at all times with Data Processors and wording in contracts will require appropriate technical and physical security. A Data Sharing Protocol will be in place at all times with other Data Controllers with which we provide personal data. Data Sharing Protocols will be reviewed every two years.

Data protection risks are informed and managed via Data Protection Impact Assessments (DPIAs) our Information Security Framework, breach and near-miss reporting lessons learned and root cause analysis, DPO monitoring activities and audits of security incidents. When appropriate, such risks are escalated to Audit and Risk Committee.

4.8 We will keep records to demonstrate compliance in our data protection activities. This includes copies of DPIAs for more risky processing and implement data protection by design as well as records to demonstrate compliance with legislation on consent.

We will deliver training and awareness programmes covering legislation, compliance, risk and other matters relating to data protection and privacy to ensure that employees are aware of and understand their responsibilities when processing personal data.

4.9 We limit our response on information in the public interest to that which is contractual in connection with the legal obligations of public authorities under the Freedom of Information Act 2000, except where we have a legal obligation.

4.10 We will maintain a manifest of CCTV cameras where we are the Data Controller. A DPIA will be conducted prior to any installations reviewed annually.

4.11 Breaches and near-breaches will be investigated by the Assistant Director of ICT or the Company Secretary so that we can notify the Information Commissioner within 72 hours and inform the Data Subjects, depending on whether these actions are appropriate.

4.12 The Assistant Director of ICT will ensure that the selection of ICT infrastructure and applications considers confidentiality, integrity and availability, that their configuration is secure, and that testing is undertaken regularly to provide assurance.

4.13 Personal data will not be transferred to countries outside the United Kingdom or European Union except where such countries have been determined to have adequate data protection provisions through a European Commission adequacy decision or there is a set of adequate safeguards with contractual terms as approved by the Information Commissioners Office (ICO) or the European Commission.

5. Legislation and Regulation

- Data Protection Act 2018 including UK GDPR; and
- Freedom of Information Act 2000.

6. Service Standards

The service standards are prescribed by legislation. We will ensure a continuous cycle of internal audit of data protection risks in liaison with the Data Protection Officer. Where risks are identified, they will be mitigated through a Data Protection Work Plan which will be reviewed annually.

7. List of related internal documents (including procedures relating to the **Policy**)

- Standard Operating Procedures for Information Governance