Havebury Housing Partnership

DATA PROTECTION POLICY

Unique Reference No	**GP016**
Date created	25th November 2020
Date for review	January 2023
Author	Assistant Director of ICT
Version Number	3
Status	FINAL
Accountable Director	Director of Resources and Company Secretary
Tenant Consultation	Tenants Forum – 7th December 2020
Equality & Diversity Impact Assessment	Low

1. Responsibility

The Board has overall responsibility for compliance with data protection legislation and this Policy. The Chair of the Audit and Risk Committee will ensure that a contract is in place for a Data Protection Officer. The Data Protection Officer will report to the Audit and Risk Committee and carry out the functions expected of that role as defined in law. 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 company members, consultative body members, agency workers, appointed agents and contractors are responsible for data protection and complying with the law 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.

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.

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 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 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 GDPR. In the case of Special Category Data, there must be an additional legal basis from Article 9 of GDPR (and where appropriate Schedule 1 of the Data Protection Act 2018) 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.

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.

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 (Subject Access Request)
- the right of rectification if data is incorrect
- the right to be informed
- the right to restrict processing

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

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. DPIAs will be performed against existing and new privacy risks on at least a three-year cycle.

- 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.

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 It is prohibited by anyone (including employees and third-parties) to use any device for storing personal data other than a Havebury encrypted device as prescribed by the Assistant Director of ICT.

4.14 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. Personal data will not be transferred to territories outside the European Economic Area (EEA) unless there are adequate safeguards.

4.15 Personal data will not be transferred to third countries that do not have adequate safeguards in place. Such arrangements will be subject to a set of Standard Contractual Clauses.

5. Legislation and Regulation

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, also referred to as General Data Protection Regulation (GDPR), or any regulation or law that is introduced on 1st January 2021 which provides equivalence to GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000

6. Service Standards

The service standards are prescribed by legislation. A set of performance reports will be maintained to demonstrate our compliance and will be reported to Management Team.

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