DATA PROTECTION

Policy Statement

1.0 Introduction

1.1 HYELM ("us", "our", "we") is a data controller.

1.2 We will do its best to comply with the law on protecting personal data as set out in particular in the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 (as amended from time to time).

1.3 We are committed to challenging discrimination and promoting equality of opportunity in every area of our work. This policy is written from an equal opportunities perspective.

1.4 This policy, and others, if requested, are available in different formats, such as languages, large print and recorded form.

2.0 Scope and Objectives

2.1 This policy sets out how we will govern and manage our data protection obligations.

2.2 This policy applies to any personal data that we process. In particular this will relate to our tenants, residents and their families, leaseholders, our staff and board members and staff of contractors and organisations that we work with. It applies not only to individuals that we are currently dealing with but also those that we dealt with previously and applicants (for example persons applying for tenancies or jobs).

3.0 Related Documents

3.1 This policy should be read in conjunction with:

- CCTV Policy.
- Data Breach Procedure.
- Data Retention Procedure.
- IT Policy.
- Privacy Notices.
- Processing Special Category Data Procedure.
- Record of Processing Activities.
- Subject Access Request Procedure.

4.0 Data Protection Principles

4.1 The data protection principles lie at the heart of how we comply with data protection legislation. In summary, they are as follows:

- Data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).
- Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).
- Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Data must be accurate and, where necessary, kept up to date (accuracy).
- Data must be 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 (storage limitation).
- Data must be 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 (integrity and confidentiality).
- We must be accountable ensuring that we can demonstrate compliance with the other principles.

5.0 Policies & Procedures for Ensuring Compliance with the Principles

5.1 To ensure that we comply with the data protection principles we have developed a number of associated policies, procedures and notices.

6.0 Privacy Notices

6.1 We have developed privacy notices which provide information about matters our processing. These include information on:

- HYELM as a data controller;
- Who personal data relates to;
- How we collect personal data;
- The personal data that we hold on, in particular, residents and visitors, commercial tenants, contractors, staff and board members;
- The purposes for which we process personal data and the lawful basis for processing that personal data;
- With whom we share personal data;
- Arrangements to make sure that data is processed securely;
- How long we retain personal data;
- Rights of data subjects;
- How to raise complaints and concerns.

7.0 Record of Processing Activities

7.1 We have a documented record which sets out a record of our processing activities as required by Article 30 of the GDPR including the purposes of processing, the data subjects and the categories of data.

8.0 Data Retention Procedure

8.1 We have a procedure for dealing with data retention. This sets out, in relation to different categories of personal data, the periods for which we retain data, the circumstances in which we may retain it for longer and the process by which we dispose of data.

9.0 Data Breach Procedure

9.1 We have a procedure for dealing with data breaches. This describes a data breach and sets out the steps that we should follow if there is a data breach.

10.0 Processing Special Category Data Procedure

10.1 We have a procedure for dealing the processing of special category data. This explains the measures that we take to ensure that we comply with our obligations under the data protection principles when processing special category personal data and data relating to criminal offences and records.

11.0 CCTV Policy

11.1 We have a policy on the purposes for which we use CCTV and the circumstances in which video may be accessed and who may access it.

12.0 IT Policy

12.1 We have a policy on Information Technology (IT) and the security measure that are in place to secure and protect data.

12.2 Our internet facing infrastructure is assessed against the Government backed Cyber Essential Scheme.

13.0 Review and Updating

13.1 We will review our arrangements over data protection to ensure compliance and that measures are effective at least every three years and more often if we make material changes and, in particular, if:

- We process data for different purposes; or
- We process data on a category or individual not previously processed.

14.0 Key Responsibilities

14.1 The Board has overall responsibilities for ensuring compliance with our legal obligations under Data Protection law.

14.2 The Company Secretary has responsibility for:

- Managing and monitoring compliance with this policy including delegating specific tasks to members of staff either by ensuring that particular aspects form part of a job description or that specific tasks are delegated.
- Ensuring that:
  - Our network and information systems are secure;
  - The data that we process within our systems is held securely with appropriate access controls;
  - Our website and online services and applications are secure;
  - The devices that we use are secure and encrypted.
- Managing and dealing with any alleged data breach including assessing the breach and its implications, notifying those affected (if required) and notifying and providing information to the Information Commissioner.
- Where any individual exercises a data subject right (e.g. a right of subject access), overseeing the handling of the request and ensuring that the request is responded to appropriately and in a timely manner.
- Arranging and ensuring that employees receive appropriate training.

15.0 Training

15.1 We will ensure that this policy is communicated to all employees at induction and that role appropriate training is provided so that staff with access to personal data understand their roles and responsibilities in relation to personal data and that, if appropriate, they receive update or refresher training, as required.