GDPR DATA PROTECTION POLICY

Introduction

Gross Hill Management Services Limited (the "**Company**") needs to gather and use certain information about individuals. These can include tenants, employees, suppliers, business contacts, and other people the organisation has a relationship with or may need to contact.

This policy describes how any personal data must be collected, handled and stored to comply with the law.

It applies to all employees of the Company and the Company as a whole. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection policy may result in disciplinary action.

This policy also applies to the Gross Hill Properties group of companies, including Sydney & London Properties and all subsidiaries and associated companies insofar as Gross Hill Management Services Limited provides administrative services to those companies.

These rules apply regardless of whether data is stored electronically on the Company's computer systems and devices (collectively **"IT systems"**), on paper or other materials.

The Company has not appointed a Data Protection Officer. It is not required for certain types of organisations with less than 250 employees. The directors have responsibility for data protection compliance within the Company. Questions about this policy, or requests for further information, should be directed to Kate Collyer (Company Secretary / Director) or, in her absence, any other director.

Definitions

"Data Subject" is a living, identified or identifiable individual about whom the Company holds Personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal data.

"Personal data" is any information that relates to an individual who can be identified from that data alone, or in combination with other identifiers we possess or can reasonably access. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it. Processing also includes transmitting or transferring Personal data to third parties.

"UK GDPR" is the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679)* as defined in the Data Protection Act 2018. Personal data is subject to the legal safeguards specified in the UK GDPR.

"Special categories of personal data" (also known as sensitive personal data) means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means personal data about an individual's criminal convictions and offences, and personal data relating to criminal allegations and proceedings.

Data protection principles

The Company is committed to the principles set out in the UK GDPR and processes personal data in accordance with the following data protection principles:

• The Company processes personal data lawfully, fairly and in a transparent manner.

• The Company collects personal data only for specified, explicit and legitimate purposes.

• The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

• The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

• The Company keeps personal data only for the period necessary for processing.

• The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised/unlawful processing, accidental loss, destruction or damage.

• The Company will not transfer personal data to another country without appropriate safeguards in place.

• The Company will make the personal data available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal data.

The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the requirements of the UK GDPR and this Data Protection Policy.

The Company will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data may be held in hard copy or electronic format, or both, and on IT systems. The periods for which the Company holds personal data are contained in its privacy notices to individuals and in the Company's **Data Retention Policy**.

The Company keeps a record of its processing activities in respect of personal data in accordance with the requirements of the UK GDPR.

Individual rights

As a Data Subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

• whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

• to whom his/her data is or may be disclosed and the safeguards that apply to such transfers;

• for how long his/her personal data is stored (or how that period is decided);

• his/her rights to rectification or erasure of data, or to restrict or object to processing;

• his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and

• whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to The Company Secretary, Gross Hill Management Services Limited, Park House, Greyfriars Road, Cardiff, CF10 3AF or enquiries@sydneyandlondon.com before the request can be processed.

The Company will respond to a request within one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, the period in which to respond may be extended by a further two months. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case and the reason for it.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge

a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

• rectify inaccurate data;

• stop processing or erase data that is no longer necessary for the purposes of processing;

• stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);

• stop processing or erase data if processing is unlawful; and

• stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to The Company Secretary, Gross Hill Management Services Limited, Park House, Greyfriars Road, Cardiff, CF10 3AF or enquiries@sydneyandlondon.com

Data security

The Company takes the security of personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Our organisational and technical measures to protect personal data are set out in our **Data Security policy**.

Data breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

Personal data may be transferred to countries outside the UK and European Economic Area ("EEA") where the third country's data protection laws have been approved as adequate and comply with any applicable cross-border transfer restrictions or other applicable safeguards are in place.

Individual responsibilities

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment or internship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

• to access only data that they have authority to access and only for authorised purposes;

• not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;

• to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

• not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

• not to store personal data on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process. All members of staff receive appropriate support and training in security matters and use of IT Systems on an ongoing basis.

Changes to this Data Protection Policy

The Company will keep this Data Protection Policy under regular review. This Data Protection Policy does not override any appliable national data privacy laws and regulations in countries with the Company operates.