DATA PROTECTION POLICY

In the following Data Protection Policy references to 'The Agency' 'The Agent' 'The Organisation' or 'The Company', The Data Protection Organiser, The Data Controller, 'we' and 'us'or 'Staff' represent one or more members of City & Town Estates Ltd.

The Agent is required to obtain relevant information about employees, clients and other individuals who contact The Company in order to operate safely and in accordance with the latest regulations. In some cases it is required by law or by referencing agencies to collect and use certain types of information in order to comply with the statutory obligations of Local Authorities and government organisations.

All information collected is safeguarded to ensure it complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 1998.

We collect only data necessary to conduct business. We ensure that The Agency treats personal information lawfully.

To comply with the requirements of the GDPR The Agency will:

- collect only the required minimum of relevant information necessary for our business;
- be transparent and provide clear information to individuals about how their personal information is used and who will use the information;
- process personal information as required by current regulation;
- make sure that all client information is kept secure;
- maintain a system to ensure that information is accurate and up-to-date;
- keep information only for as long as is necessary for legal or regulatory reasons or for legitimate organisational purposes;
- treat all individuals' rights in accordance with the rules defined in the GDPR.

Information Commissioners Office (ICO)

The Agent is registered with the Information Commissioner as a data controller and/or processor to process personal data. The registration certificate is available on request.

Basics of Data Protection

All personal data will be processed safely and lawfully.

The regulator provides and advises The Agency on the main requirements for transparency relevant to our industry.

Any data needed at the time will only be collected for specified and legitimate reasons.

Personal data collected will be adequate, relevant and limited to what is necessary for processing. The Data Protection Organiser is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

We will ensure that any data obtained excessively or that is not specifically required by The Agency is securely deleted or destroyed as required.

Other Considerations

Personal data must be accurate and kept up-to-date.

We monitor and make sure that data that is kept for a long time is reviewed and updated as necessary. Any data that is inaccurate or likely to be inaccurate will be removed.

Individuals who have provided information about themselves are also responsible for ensuring that their data held by The Agency is accurate and up-to-date. Any data submitted by an individual to The Company will be assumed to be accurate at the time of receipt and accepted in good faith.

Clients, customers, contractors or other individuals should notify The Agency of any changes in their personal information to ensure data is kept up-to-date. The Agency will ensure that any notification of changes to personal information is implemented.

All Staff are responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up-to-date. This will take into consideration the volume of data collected, the speed with which it might change and any other relevant factors.

The Company will review all personal data processed by The Agency at least once a year.

If The Agent has provided inaccurate or out of date personal information to a third party our Staff is responsible for informing the third party that the information is inaccurate and/or out-of-date and for advising them that the information should no longer be used. Our Staff will also ensure that any corrections to personal information are passed on to the third party.

Personal Data Considerations

Personal data is kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will either be minimised or deleted altogether.

Personal data will only be kept in accordance with the retention of records procedure and it will be deleted when it is time to do so.

Only data specifically approved for retention that exceeds the allowed retention period may be kept for longer. Personal data will be processed in a manner that ensures its security.

Particular measures will be taken to avoid unauthorised or accidental loss of personal data.

Safeguards

The Data Controller considers the following:

- the country or territory of origin and destination of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee including relevant codes of practice and international obligations.

Accountability

The GDPR requires that The Data Controller is responsible for ensuring compliance with the requirements of the GDPR.

Data subjects' rights

Under Data Protection legislation, data subjects have the following rights with regard to their personal information:

- the right to be informed about the collection and use of their personal data;
- the right to access personal data and supplementary information;
- the right to have inaccurate personal data rectified, or completed if it is incomplete;
- the right to erasure (to be forgotten) in certain circumstances;
- the right to restrict processing in certain circumstances;
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services;
- the right to object to processing in certain circumstances;
- rights in relation to automated decision-making and profiling;
- the right to withdraw consent at any time (where relevant);
- the right to complain to the Information Commissioner.

Consent

The Agency understands 'consent' to mean that it has been explicitly and freely given, that it is specific, informed, and is an unambiguous indication of the data subject's wishes by which he or

she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

In addition, The Agency understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrates active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely by The Agency using standard consent documents.

Data Security

All The Agency Staff are responsible for any personal data which The Agency holds. They must keep it secure and ensure that it is not disclosed under any circumstances to any third party unless that third party has been specifically authorised by The Agency to receive that information and has entered into a Data Processing Agreement, for example a referencing company acting on our behalf.

All personal data is accessible only to those who need to use it and access will only be granted in line with the IT Security and Data Access Policy. Judgments based upon the sensitivity and value of the information in question will be made, but personal data is kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised it is password protected in line with the IT Security and Data Access Policy; and
- computer screens are not visible except to authorised Staff.

Any records, whether stored electronically or on paper will not left where they can be accessed by unauthorised personnel and will not removed from business premises without explicit authorisation when Staff are specifically authorised to process data off-site. As soon as records are no longer required for day-to-day operations they will be secured according to The Company's internal procedures.

Personal data will only be deleted or disposed of in line with the Data Retention Procedure Retention of Records. Manual records that have reached their retention date will be destroyed and disposed of as 'confidential waste'. Hard drives of redundant PCs will be removed and immediately destroyed as required by the Data Handling Procedure before disposal.

Rights of access to data

Data subjects have the right to access any personal data (that is, data about them) which is held by The Agency in electronic formats and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by The Agency and information obtained from third party organisations about that person.

Disclosure of data

The Agency will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and in certain circumstances, the Police. All Staff must exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of The Agency's business.

The GDPR permits a number of exemptions where certain disclosure without consent is permitted as long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- for the prevention or detection of crime including the apprehension or prosecution of offender;
- for the assessment or collection of taxes;
- to discharge regulatory functions (health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual regarding life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by The Data Protection Controller.

Retention and disposal of data

Personal data is not retained for longer than is required in accordance with data protection reglulation. Some data may be be kept for longer periods than other data.

Disposal of records

Personal data is disposed of in a way that protects the client and other individuals, for example, permanent file deleting, shredding, responsible disposal as confidential waste.

E-mail and Internet privacy

The inappropriate use of e-mail and the internet by employees for example, using the internet for non-work purposes could have significant consequences for The Agency. This could be in terms of:

- embarrassment or damage to The Agency's reputation;
- loss of productivity;
- increased risk of liability and legal action for example, for sexist or racist e-mails;
- increased virus risk.

To avoid inappropriate usage, The Company has introduced electronic security safeguards which include firewall checks, guarantees and management of e-mail attachments.

Staff will be kept fully informed about overall information security procedures and the importance of their role in these procedures. Manual filing systems are held in secure locations and only authorised employees can access them.