DATA PROTECTION POLICY 2018

JCF PROPERTY MANAGEMENT LTD

Company Name:	JCF Property Management Ltd ('the Company')
Document:	Data Protection Policy
Topic:	General Data Protection Regulations
Date:	18/05/2018

Table of Contents

Introduction

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process that data.

As a property management business, the Company collects and processes personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws.

Definitions

In this policy the following terms have the following meanings:

'*consent*' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of *personal data* relating to him or her;

'*data controller*' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

'*data processor*' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'*personal data*' means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'supervisory authority' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised (with the exception of chapter and paragraph titles, and the Table of Content) throughout this policy to remind the reader that they are defined terms.

Data processing under the Data Protection Laws

The Company processes *personal data* in relation to individual client contacts and its own staff, and is a *data controller* for the purposes of the Data Protection Laws.

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Accounts and records; and
- Administration and *processing* of *personal data* for the purposes of property management services, including *processing* using software solution providers and back office support.

The data protection principles

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* is processed;
6. 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, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

Legal bases for processing

The Company will only process personal data where it has a legal basis for doing so. Where the Company does not have a legal basis for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring personal data to any third party (such as suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party {such as software solutions providers and back office support}), the Company will establish that it has a legal basis for making the transfer.

Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

- data minimisation (i.e. collecting unnecessary data or keeping it longer than is necessary); and
- IT security.

Rights of the Individual

The Company shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

Privacy notices

Where the Company collects personal data from the individual, the Company will give the individual a privacy notice at the time when it first obtains the personal data.

Where the Company collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month of the data being collected. If the Company intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data is first disclosed (if not issued sooner).

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

Rectification

The individual or another data controller at the individual's request has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning the individual.

If the Company has given the personal data to any third parties, it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

Erasure

The individual or another *data controller* at the individual's request, has the right to ask the Company to erase that individual's *personal data.*

If the Company receives a request to erase *personal data*, it will ask the individual if he/she wants his/her *personal data* to be removed entirely or whether he/she is happy for his/her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased, so the individual may be contacted again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If the Company has given the *personal data* to any third parties, it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate

effort. Those third parties should also erase the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the erasure has occurred.

Restriction of processing

The individual or a *data controller* at the individual's request, has the right to ask the Company to restrict its *processing* of that individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes erasure of the *personal data*;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the
- *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict processing of the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also restrict processing of the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the restriction of processing has occurred.

Data portability

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit that data to another data controller in circumstances where:

- The processing is based on the individual's consent or a contract; and
- The processing is carried out by automated means.

Where feasible, the Company will send the personal data to a named third party on the individual's request.

Object to processing

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data being used for direct marketing.

Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature, the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

Automated decision making

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller*
- and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

The Company will not carry out any automated decision-making using the *personal data* of a child.

Personal Data Breaches

Reporting personal data breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

Personal data breaches where the Company is the data controller

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

Personal data breaches where the Company is the data processor

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

Communicating personal data breaches to individuals

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to individually tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

The Human Rights Act 1998

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

Complaints

If you have a complaint or suggestion about the Company's handling of personal data then please contact the person whose details are listed in the Appendix to this policy.

Alternatively, you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

Appendix

Those responsible for:

- Adding, amending or deleting *personal data*;
  ALL EMPLOYEES OF JCF PROPERTY MANAGEMENT LTD

- Responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision making processes;
  ALL EMPLOYEES OF JCF PROPERTY MANAGEMENT LTD

- Reporting data breaches and dealing with complaints
  PAUL ALFIERI (DIRECTOR, FINANCE & ADMINISTRATION)
  DAVID GRAVES (MANAGING DIRECTOR)
  STEWART WHITE (DIRECTOR)

The lawfulness of *processing* conditions for *personal data* are:

1. *Consent* of the individual for one or more specific purposes.
2. *Processing* is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
4. *Processing* is necessary to protect the vital interests of the individual or another person.
5. *Processing* is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the *data controller*.
6. *Processing* is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of *personal data*, in particular where the individual is a child.