DATA PROTECTION POLICY

This Policy has been approved and authorised by:

NAME:	Duncan Pate
POSITION:	Managing Director
REVIEW DATE:	May 2018
SIGNATURE:	

Date of Implementation:	25th May 2018
ICO Registration No:	Castles Property Services Ltd Z8781767 Castles Letting & Management Ltd ZA364748

CONTENTS

1. **Introduction**
2. **Definitions**
3. **Data Protection Principles**

4. **Lawful, Fair, and Transparent Data Processing**
5. **Processing for Specified, Explicit and Legitimate Purposes**
6. **Adequate, Relevant and Limited Data Processing**
7. **Accuracy of Data and Keeping Data UpToDate**
8. **Timely Processing**
9. **Secure Processing**
10. **Accountability**
11. **Privacy Impact Assessments**
12. **The Rights of Data Subjects**
13. **Keeping Data Subjects Informed**
14. **Data Subject Access**
15. **Rectification of Personal Data**
16. **Erasure of Personal Data**
17. **Restriction of Personal Data Processing**
18. **Data Portability**
19. **Objections to Personal Data Processing**
20. **Automated Decision-Making**
21. **Profiling**
22. **Personal Data**
23. **Data Protection Measures**
24. **Organisational Measures**
25. **Data Breach Notification**

1. Introduction

This document outlines the policy of Castles Property Services Ltd & Castles Letting & Management Ltd with regards to handling our data protection obligations and the rights of customers to comply with the General Data Protection Regulations ("GDPR").

We are committed to compliance with the GDPR. We will as a minimum meet the letter of the law, but wherever possible we will also look to exceed it.

This policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by us, our employees, sub-agents, contractors, or other parties working on our behalf to ensure the correct, lawful, and fair handling of all personal data.

2. Definitions

Customers	Data Subjects
Data Subjects	Any person we obtain personal information from, including property sellers, buyers, landlords, applicants and tenants.
Data Controller	a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
GDPR	The General Data Protection Regulations
ICO	Information Commissioners Office

Personal Data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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.
The Company/We/Us/Our	Castles Property Services Ltd & Castles Letting & Management Ltd, Turnpike House, 1208/1210 London Road, Leigh On Sea, Essex SS9 2UA

3. **Data Protection Principles**

3.1 We aim to ensure compliance with the principles of the Regulations and as such all personal data must be:

a) Processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) Accurate and, where necessary, 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 they are processed, is erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) 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.

4. **Lawful, Fair, and Transparent Data Processing**

4.1 GDPR requires that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. To ensure we are compliant we will only process data where:

a) The data subject has given consent to the processing of his or her personal data

for one or more specific purposes;

b) It is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) It is necessary for compliance with a legal obligation to which the controller is subject;

d) It is necessary to protect the vital interests of the data subject or of another natural person;

e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) It is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

5. Processing for Specified, Explicit and Legitimate Purposes

5.1 We collect and process the personal data set out in Section 22 below. This may include personal data received directly from data subjects when we directly interact with them.

5.2 It may also include data received from third parties. Third parties include, but are not restricted to – Rightmove.co.uk, Onthemarket.com (Agents Mutual) Rent4Sure Ltd, Tenant Shop, Tenancy Deposit Scheme

5.3 We only process personal data for specific purposes –

a) As set out in Section 22 of this Policy; &

b) For other purposes expressly permitted by GDPR; &

c) For the purposes meeting any statutory obligation we have; &

d) Complying with any other legal obligation.

5.4 The purposes for which we process personal data will be informed to data subjects –

a) Within our written Terms of Business;

b) On our Website;

c) Verbally at the time information is taken;

d) As soon as possible after collection where it is obtained from a third party.

6. Adequate, Relevant and Limited Data Processing

We only collect and process personal data that is adequate, relevant and limited for to the extent necessary to provide the service we agreed or for the specific purpose(s) informed to data subject.

7. Accuracy of Data and Keeping Data Up-To Date

We will ensure that all personal data collected and processed is accurate when collected. Then reviewed at intervals thereafter to ensure it remains up to date. Appropriate steps will be taken, in a timely manner, to amend or erase inaccurate or out-of-date data.

8. Timely Processing

We will not keep personal data for any longer than is necessary, considering the purposes for which that data was originally collected and processed. When the data is no longer required appropriate steps will be taken, in a timely manner, to erase the data.

9. Secure Processing

We will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which will be taken are provided in Parts 23 and 24 of this Policy.

10. Accountability

10.1 Our Data Protection Officer is Duncan Pate

10.2 We will retain written internal records of all personal data collected, held and processed, which will include the following information:

a) The details of any third-party data controllers any third parties that will receive personal data from us;

b) The purposes for which we process personal data;

c) Details of the categories of personal data collected, held, and processed;

d) Details of how long we will retain personal data;

e) Details of the measures we take to ensure security of personal data.

11. Privacy Impact Assessments

11.1 We will carry out Privacy Impact Assessments when and as required under the GDPR. Privacy Impact Assessments will be managed by Castles Property Services Ltd & Castles Letting & Management Ltd. and will address the following areas of importance:

a) The purpose for which personal data is being held and processed and the processing operations that will be carried out;

b) Confirmation of the legitimate interests we are pursuing;

c) An assessment of the necessity and proportionality of the data processing, considering the purpose for which it is being processed;

d) An assessment of the risks posed to individual data subjects and details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of

personal data, sufficient to demonstrate compliance with the GDPR.

12. The Rights of Data Subjects

12.1 The GDPR sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the 'right to be forgotten');

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

13. Keeping Data Subjects Informed

13.1 We will ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Company

b) The identity of our Data Protection Officer

c) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

d) Where applicable, the legitimate interests we justify its collection and processing;

e) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

f) Where the personal data is to be transferred to one or more third parties, details of those parties;

g) Details of the length of time the personal data will be held by us (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right to withdraw their consent to processing of their personal data at any time;

j) Details of the data subject's right to complain to the ICO;

k) Details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences for the data subject for failing to provide it;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any

consequences.

13.2 The information set out above in Section 12.1 will be provided to the data subject –

a) At the time of collection where we obtain the data ourselves; or

b) At the time of the first communication, if the personal data is used to communicate with the data subject, or

c) Before the personal data is disclosed, if it is to be disclosed to another party; or

d) In any event, not more than one month after the date we obtained the personal data.

14. Data Subject Access

14.1 A data subject may make a Subject Access Request (SAR) at any time to find out more about the personal data we hold about them. We will normally respond to a SAR within one month of receipt, or two months for complex and/or numerous requests. We will inform the data subject of the need for the extension, if appropriate.

14.2 All SAR received must be forwarded to Duncan Pate or Penny Pate

14.3 We do not charge for the handling of normal SARs, but we reserve the right to charge a reasonable fee for additional copies of information already supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

15. Rectification of Personal Data

15.1 If we are informed by the data subject that personal data we hold is inaccurate or incomplete, and they request correction we will do so and confirm our actions with the data subject, normally, within one month of receipt the data subject's notice, but this may be extended to two months in complex situations We will inform the data subject of the need for the extension, if appropriate.

15.2 Where any disclosure of inaccurate data has been made to a third party we will advise the third party of the correction.

16. Erasure of Personal Data

16.1 Data subjects can request that we erase the personal data we hold about them in the following circumstances:

a) It is no longer necessary for us to hold that personal data for the purpose it was originally collected or processed;

b) The data subject wishes to withdraw their consent to us to hold and process their personal data;

c) The data subject objects to us holding and processing their personal data. Unless there is an overriding legitimate interest allowing us to continue to do so. (see Section 12 and 17 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased so that we can comply with a particular legal obligation**.**

16.2 Unless we have reasonable grounds to refuse to erase personal data, all requests for erasure will be complied with, and the data subject informed within one month of receipt of the data subject's request, but this may be extended to two months in complex situations We will inform the data subject of the need for the extension, if appropriate.

16.3 If any personal data that is to be erased in response to a data subject request has been disclosed to third parties, we will inform those parties of the erasure, unless it is impossible or would require disproportionate effort to do so.

17. Restriction of Personal Data Processing

17.1 Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

17.2 If any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it, unless it is impossible or would require disproportionate effort to do so.

18. Data Portability

18.1 We do not process personal data using automated means.

18.2 Where data subjects have given their consent to us to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between us and the data subject, data subjects have the legal right under the GDPR to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

18.3 To facilitate the right of data portability, we will make available all applicable personal data to data subjects in the following format:

a) **Electronic copies**

b) **Hardcopy printed documents**

18.4 If requested by a data subject, personal data will be sent directly to another data controller, if it is possible.

18.5 All requests for copies of personal data will be provided within one month of receipt, or two months for complex and/or numerous requests. We will inform the data subject of the need for the extension, if appropriate.

19. Objections to Personal Data Processing

19.1 Data subjects have the right to object to us processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).

19.2 Where a data subject objects to us processing their personal data based on its legitimate interests, we will cease such processing forthwith, unless it can be

demonstrated that we have legitimate grounds for such processing and these override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

19.3 Where a data subject objects to us processing their personal data for direct marketing purposes, we will cease such processing forthwith.

20. **Automated Decision-Making**

20.1 In the event we use personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, they have the right to challenge those decisions under GDPR. They can request human intervention, express their own point of view, and obtain an explanation of the decision from us.

20.2 The right described in 20.1 does not apply where:

a) The decision is necessary for the entry into, or performance of, a contract between us and the data subject;

b) The decision is authorised by law;

c) The data subject has given their explicit consent.

21. **Profiling**

20.1 Where we use personal data for profiling purposes, then:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected will be implemented; and

d) All personal data processed for profiling purposes will be secured in order to prevent discriminatory effects arising out of profiling (see Parts 23 and 24 of this Policy for more details on data security).

21. **Personal Data**

22.1 The following personal data may be collected, held, and processed by us in order **to market directly to potential customers:**

a) Name

b) Home address

c) Contact telephone numbers

d) Email address

22.2 The following personal data may be collected, held, and processed by us **from potential buyers and potential tenants:**

a) Name

b) Home address

c) Contact telephone numbers

d) Email address

e) Their current property situation

f) Their property purchase/rental budget

g) Their current property purchasing or renting financial position

h) Their property purchase/rental preferences

i) Copies of documents to confirm that funds are available to purchase properties

1.3 The following personal data may be collected, held, and processed by us **from our property selling clients:**

a) Name

b) Home address

c) Contact telephone numbers

d) Email address

e) Their properties value

f) Full details of the property to be marketed

g) Photographs of the property to be marketed

h) Alarm codes and other security information where we are conducting viewing

22.4 The following personal data may be collected, held, and processed by us **from our landlord clients:**

a) Name

b) Home address

c) Contact telephone numbers

d) Email address

e) Their properties rental value

f) Full details of the property to be marketed

g) Photographs of the property to be marketed

h) Alarm codes and other security information where we are conducting viewing

i) Official or other photographic identity confirmation

j) Copies of appropriate documents to confirm home address

22.5 The following personal data may be collected, held, and processed by us **from applicants for tenancies and tenants:**

a) Name

b) Home address

c) Contact telephone numbers

d) Email address

e) The information required to complete a tenancy application (contained in a

separate document Tenants Information Guide)

22.6 The following personal data may be collected, held, and processed by us **from seller clients and buyers to meet our obligations under Money Laundering Regulations:**

a) Name

b) Date of Birth

c) Home address

d) Period they have lived at their current property

e) Official photographic identity confirmation

f) Copies of appropriate documents to confirm home address

g) Copies of documents to confirm that funds are available to purchase properties

22.7 The following personal data may be collected, held, and processed by us **from Tenants to meet our obligations under the Immigration Act 2014:**

a) Name

b) Date of Birth

c) Official photographic identity confirmation

23. **Data Protection Measures**

23.1 All our employees, agents, contractors, or other parties working on our behalf must comply with the following when working with personal data:

a) All emails must be encrypted

b) Where any personal data, including copies, is to be erased or otherwise disposed of for any reason, it should be deleted and disposed of in a permanent and secure manner. Hardcopies should be shredded, and electronic copies should be professionally deleted;

c) Personal data may be transmitted over secure networks only;

d) Facsimile transmission of personal data is not permitted;

e) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent by an appropriate delivery service after considering the type of data and security of delivery:

f) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on our behalf requires access to any personal data that they do not already have access to, such access should be formally requested from **Duncan Pate Managing Director**

g) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored using an appropriate level of security;

h) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on our behalf without, our appropriate consent;

i) Personal data must always be handled with care and should not be left

unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

j) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

k) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to us or otherwise, without our appropriate consent and in the event of such consent, strictly in accordance with all instructions and limitations described at the time the consent is given, and for no longer than is absolutely necessary**;**

l) No personal data should be transferred to any device personally belonging to an employee;

m) Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf with our appropriate consent;

n) All electronic copies of personal data should be stored securely using passwords and data encryption**;**

o) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All the software we use requires passwords;

p) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

q) All personal data stored electronically should be backed up every week with backups stored on USB.

r) All backups are encrypted using symmetric encryption. (Deslock)

24. Organisational Measures

24.1 We will ensure that the following measures are taken when collecting, holding, and processing personal data:

a) All employees, agents, contractors, or other parties working on our behalf will be made fully aware of both their individual responsibilities and our responsibilities under the GDPR and under this Policy, and they will be provided with a copy of this policy;

b) Only employees, agents, sub-contractors, or other parties working on our behalf that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by us;

c) All employees, agents, contractors, or other parties working on our behalf handling personal data will be appropriately trained;

d) All employees, agents, contractors, or other parties working on our behalf

handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed;

f) The performance of employees, agents, contractors, or other parties working on our behalf handling personal data will be regularly evaluated and reviewed;

25. **Data Breach Notification**

25.1 All personal data breaches must be reported immediately to **Duncan Pate or Penny Pate**

25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), we will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

25.3 If a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, we will ensure that all affected data subjects are informed of the breach directly and without undue delay.

25.4 Data breach notifications will include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of **Duncan Pate or Penny Pate**

d) The likely consequences of the breach;

e) Details of the measures we have taken or proposed to be taken to address the breach including, where appropriate, measures to mitigate its possible adverse effects.