GENERAL DATA PROTECTION REGULATION (EU) 2016/679 ("the GDPR")

PRIVACY POLICY

MAY 2018

CONTENTS

1. Introduction p3
2. Legislation p4
3. Data p5
4. Processing of Personal Data p6-9
5. Data Sharing p10-11
6. Data Storage and Security p12
7. Breaches p13-14
8. Data Protection Officer p15
9. Data Subject Rights p16-19
10. Privacy Impact Assessments ("PIAs") p20-21
11 Archiving, Retention and Destruction of Data p21
12. Changes to the Privacy Policy p21
13. Related Documents p22

1. Introduction

Waverley Housing is committed to ensuring the secure and safe management of data held by it in relation to customers, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

We need to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that we have a relationship with. We manage a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

This Policy sets out our duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that we process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of Personal Data and privacy as a consequence of the United Kingdom leaving the European Union.

3. Data

3.1

We hold a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by us is detailed within the Fair Processing Notice provided.

3.1.1

"Personal Data" is that from which a living individual can be identified either by that data alone or in conjunction with other data held by us.

3.1.2

We also hold Personal Data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

4.1

We are permitted to process Personal Data on behalf of data subjects provided it is done on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof)
- Processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject
- Processing is necessary for our compliance with a legal obligation including any regulatory requirements
- Processing is necessary to protect the vital interests of the data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of our official authority or
- Processing is necessary for the purposes of legitimate interests.

4.2 Fair Processing Notices

4.2.1

We have produced Fair Processing Notices (FPN) which we require to provide to all our customers, employees and others whose Personal Data is held by us. That FPN must in accordance with GDPR be provided from the outset of processing their Personal Data and sets out the data processed by us and the basis for that processing. If you have any queries regarding the terms of the FPN provided, you should contact us.

4.3 Employees/Board Members

4.3.1

Employee/Board Members Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by us. Details of the data held and processing of that data is contained within the Employee/ Board Members Fair Processing Notice which will be provided to Employees and Board Members at the same time as their Contract of Employment or in the case of Board Members, at their induction. All existing staff and Board Members have been furnished with a copy of the FPN.

4.3.2

A copy of any Employee or Board Member's Personal Data held by us is available upon written request to Margaret Hogg, Business Support Manager. A Data Subject Access request form should be completed by the Employee or Board Member for this purpose.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by us when processing Personal Data. It shall be used where no other alternative ground for processing is available. In the event that we require to obtain consent to process a data subject's Personal Data, we shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that we process Special Category Personal Data or Sensitive Personal Data, we shall do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity and
- Processing is necessary for reasons of substantial public interest.

5. Data Sharing

5.1

We share data with various third parties for numerous reasons in order that our day to day activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third parties with Data Protection laws, we will require the third party organisations to enter in to an Agreement with us governing the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data Sharing

5.2.1

Personal Data is from time to time shared internally across our staff and third parties who require to process Personal Data that we process as well. Both us and the third party will be processing that data in our individual capacities as data controllers.

5.2.2

Where we share in the processing of Personal Data with a third party organisation, it shall require the third party organisation to enter in to a Data Sharing Agreement with us in accordance with the terms of the model Data Sharing Agreement - see 13 Related Documents.

5.3 Data Processors

A data processor is a third party entity that processes Personal Data on our behalf, and are frequently engaged if certain of our work is outsourced (e.g., maintenance and repair works).

5.3.1

A data processor must comply with Data Protection laws. Our data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered.

5.3.2

If a data processor wishes to sub-contract their processing, our prior written consent must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.3

Where we contract a third party to process Personal Data held by us, we shall require the third party to enter in to a Data Protection Addendum with us in accordance with the terms of the model Data Protection Addendum- see section 13 Related Documents.

6. Data Storage and Security

All Personal Data held by us must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Personal Data should not be left where unauthorised personnel can access it. When the Personal Data is no longer required it will be disposed of by the Employee or Board Member so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then it shall be stored securely and disposed of in accordance with our Data Retention Periods.

6.2 Electronic Storage

Personal Data stored electronically is also protected from unauthorised use and access. Personal Data is password protected or encrypted when sent externally to our data processors or those with whom we have entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media content is encrypted and is stored securely at all times when not being used. Personal Data will be securely stored on designated drives and servers.

7. Breaches

7.1

A data breach can occur at any point when handling Personal Data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

7.2 Internal Reporting

We take the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Data Protection Officer must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s)

- We will seek to contain the breach by whatever means available

- The Data Protection Officer must consider whether the breach is one which requires to be reported to the Information Commissioner's Office and data subjects affected and do so in accordance with this clause 7

- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

7.3 Reporting to the Information Commissioner's Office

The Data Protection Officer will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office within 72 hours of the breach occurring. The Data Protection Officer must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer

8.1

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over our compliance with Data Protection laws. We have elected to appoint a Data Protection Officer whose details are noted on our website and contained within the Fair Processing Notices.

8.2 Our Data Protection Officer will be responsible for:

8.2.1

monitoring our compliance with Data Protection laws and this Policy

8.2.2

co-operating with and serving as our contact for discussions with the Information Commissioner's Office

8.2.3

reporting breaches or suspected breaches to the Information Commissioner's Office and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

9.1

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the Personal Data held by us about them, whether in written or electronic form.

9.2

Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to our processing of their data. These rights are notified to our tenants and other customers in our Fair Processing Notice.

9.3 Subject Access Requests

Data Subjects are permitted to view their data held by us upon completing a written Subject Access Request form. Upon receipt of a request by a data subject, we must respond to the Subject Access Request within one month of the date of receipt of the request.

9.3.1

We must provide the data subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.

9.3.2

Where the Personal Data comprises data relating to other data subjects, we must take reasonable steps to obtain consent from those data subjects to the disclosure of that Personal Data to the data subject who has made the Subject Access Request, or

9.3.3

where consent is not given by the other data subject, we may provide this by redaction of their Personal Data or determine not to provide where any content may still allow identification of that data subject withholding consent or

9.3.4

where we do not hold the Personal Data sought by the data subject, we must confirm that we do not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 The Right to be Forgotten

9.4.1

A data subject can exercise their right to be forgotten by completing our Data Subject Rights Form to request that we erase the data subject's Personal Data in its entirety.

9.4.2

Each request received by us will require to be considered on its own merits and legal advice may require to be obtained in relation to such requests from time to time. The Data Protection Officer will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

9.5 The Right to Restrict or Object to Processing or to have data rectified

9.5.1

A data subject may request that we restrict our processing of the data subject's Personal Data, or object to the processing of that data or to have specific Personal Data rectified.

Any request must be by completion of our Data Subjects Rights Form.

9.5.1.1

In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature, and if we receive such a written request to cease processing for this purpose, then we will do so immediately.

9.5.2

Each request received by us will require to be considered on its own merits and legal advice may require to be obtained in relation to such requests from time to time.

The Data Protection Officer will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

10.1

These are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 We shall:

10.2.1

Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data and

10.2.2

In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data.

10.3

We will require to consult the Information Commissioner's Office in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Data Protection Officer within five (5) working days.

11. Archiving, Retention and Destruction of Data

We cannot store and retain Personal Data indefinitely. We will ensure that Personal Data is only retained for the period necessary. We shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within our Data Retention Periods - see section 13 Related Documents.

12. Changes to our Privacy Policy

Waverley Housing reserves the right to amend this Policy at any time and undertakes to carry out a 3-yearly review of the Policy in accordance with our Policy Review Listing.

13. Related Documents

1: Fair Processing Notice (Employees/Board Members)
Fair Processing Notice (others)
(A copy of the relevant Fair Processing Notice will be provided at source of collection of data)

The undernoted documents are available upon request or from our website www.waverley-housing.co.uk.

2: Roles and Responsibilities

3: Model Data Sharing Agreement

4: Model Data Protection Addendum

5: Data Retention Periods

waverley housing

51 North Bridge Street
Hawick • TD9 9PX
T: 01450 364200
E: info@waverley-housing.co.uk
www.waverley-housing.co.uk

follow us on....

@WaverleyHousing

To request a larger print version of this document please call 01450 364200

HAPPY TO TRANSLATE

Scottish Charity No. SC026231 Companies House Registration No. 115066 Property Factors Reg No. PF000271