DATA PROTECTION POLICY

Policy Statement

Westfield Housing Association is committed to a policy of protecting the rights and privacy of individuals, Board, voluntary and community group members, staff and others in accordance with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR). Any breach of the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) or this Data Protection Policy is considered to be an offence and in that event, disciplinary procedures apply.

The Association is registered as a data controller with the Information Commissioner's Office (ICO).

1. Purpose

1.1 This policy sets out the approach of Westfield Housing Association to protecting the privacy of ***data subjects*** (our customers, board members and staff) and their data and meeting requirements of data protection law. This outlines the measures in place to demonstrate our accountability for upholding the privacy of data.

1.2 The implications of non-conformance with the data protection legislation to us as a business are:-

- Reputational damage to us – especially a lack of trust from our customers.

- Intervention and fines administered by the Information Commission Office (there are two tiers of administrative fines; (i) Up to £10 million euros or 2% of annual turnover; or (ii) up to 20 million euros or 4% of annual turnover).

- Regulatory downgrade from the Regulator of Social Housing.

2. Definitions

Data subject - A living individual who is the subject of personal data.

Personal data - Data relating to an identifiable person.

Processing data - Performing actions on data (collecting, using, storing, sharing).

Data controller - Determines the purpose/s for which the data is collected.

Data processor - Processes data on behalf of the controller - only uses the data for what the controller has determined.

Special Category Data - Data that could cause a significant risk to an individual's fundamental rights & freedoms e.g. unlawful discrimination. The General Data Protection Regulation lists these as:

- Race
- Ethnic Origin
- Political Beliefs
- Religious Beliefs
- Trade Union Membership
- Genetics
- Biometrics (Where used for identification)
- Health
- Sex Life or orientation

Personal Data Security Breach – an incident that has affected the confidentiality, integrity or availability of personal data. This could be when personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Information Commissioners Office (ICO) – the ICO is the UK's Supervisory Authority. The role of the ICO is to ensure we are complying with our data protection requirements and taking appropriate action when we are not.

3. Responsibilities

3.1 **Board** – to approve this policy and to receive reports on data security breaches where there is an obligation to report to the ICO.

3.2 **Chief Executive Officer** – overall responsibility for ensuring compliance with this policy (and other data protection policies). Leads on ***Personal Data Security Breach*** investigations and informs ICO about breaches where appropriate.

3.3 **Data Protection Information Officer (DPIO)** – Although the Association does not meet the threshold for requiring a mandatory DPIO we do have a voluntary DPIO. The DPIO role is the lead staff member for data protection. The DPIO ensures our policies are up to date and being adhered to and ensures staff and volunteers have appropriate training and ensures the rights of ***data subject*** are upheld.

3.4 **Property Services Officer** – has responsibility in ensuring contracts are compliant with data protection legislation.

3.5 **All Board Members and Employees**

- have responsibility to ensure they are compliant with our privacy and data protection policies and to report any breaches within 48 hours to the CEO or Chairman. The Data Protection Information Officer (DPIO) should provide a report identifying the cause of the breach and evaluate the impact of the breach.

- Are responsible to ensure they 'cleanse their area of responsibility at least annually in line with the guidelines set out in the National Federation's Document Retention for Housing Association document and government rules and legislation.

4. Legal Framework

There are three key pieces of data protection legislation:

4.1 ***General Data Protection Regulation (GDPR)*** – this came into force on 25th May 2018 and replaced the Data Protection Act 1998. This is an EU regulation, which means it is automatically adopted by each member of the EU. The GDPR sets out the main requirements for data protection across the EU but did leave some areas for local determination by member states.

4.2 ***Data Protection Act 2018*** - covers the areas in the GDPR for member states to determine locally.

4.3 ***Privacy and Electronic Communications Regulations*** give specific rights to individuals in relation to the use of electronic communications (e.g. cookies and marketing calls).

5. Key Principles

5.1 We are committed to safeguarding the privacy of ***data subjects*** (our customers, board members and staff) and upholding their rights in relation to data protection.

5.2 We process data in line with the principles laid out in the GDPR.

5.3 We ensure our policies are compliant with data protection legislation.

5.4 We will adopt the ICO codes of practice where practicable and relevant to our business.

5.5 We will ensure all staff receive appropriate training for their role.

5.6 We will ensure all personal data breaches are investigated and, where appropriate, report to the ICO within 72 hours. The Association's CEO and Chairman will also be notified of all breaches.

6. Accountability and Governance

6.1 The requirements and accountabilities to comply with this policy apply to all our current employees, including where necessary, members, volunteers, Board members, consultants, contractors or third parties engaged to carry out services or functions on our behalf.

6.2 The Association's Board is ultimately responsible for compliance with the requirements of data protection legislation.

6.3 We have a voluntary Data Protection Information Officer who is responsible for ensuring this policy and other relevant data protection policies are kept up-to-date, staff are trained and any non-compliances are managed appropriately.

6.4 We have clear Privacy Notices for board members, staff and all our customers. This informs ***data subjects*** of*:*

- The name and contact details of our organisation
- The contact details of our data protection officer
- The purposes and lawful basis of the processing
- The legitimate interests for the processing (if applicable)
- What data we obtain from third parties and who we obtain it from
- What data we share and who we share data with
- Where we store their personal data
- The retention periods for the personal data
- The rights of ***data subjects*** under the GDPR
- Details of the existence of automated decision-making, including profiling (if applicable).

6.5 **Personal Data Security Breaches** of this policy will be reported to the Board.

6.6 The GDPR requires us as a ***Data Controller*** to process personal data in accordance with the six data protection principles in relation to the running of our business and delivering our services. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

In addition Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

7. Rights of the data subject

7.1 We ensure that we comply with the rights of the ***data subject. These rights are:***

- The right to be informed – we have a privacy notice that informs ***data subjects*** what data we process, why we process this, who we share it with and how long we will retain it.

- The right of access – we ensure ***data subjects*** are able to access their personal data.

- **The right to rectification** - The GDPR provides the right for individuals to make a request to us for the rectification of their personal data, which they can do if they wish by completing our form. They also have the right to have incomplete personal data completed, including by means of their providing a supplementary statement. An employee may ask us to correct personal details such as their home address or mobile phone number.

Although there's no definition of "inaccurate" in the **GDPR**, the **Data Protection Act 2018** defines this term, in relation to personal data, as being "incorrect or misleading as to any matter of fact". We may decline the request if the data is factually correct and not misleading, even though the employee might not agree with the line manager's opinions.

- **The right to erasure** – we delete ***personal data*** when a ***data subject*** requests it (although this is not an absolute right and the GDPR sets out where this right does not apply).

- **The right to restrict processing** – we only use the data for the purposes that are laid out in our privacy notice. We will restrict our processing of ***personal data*** where a ***data subject*** has the right to restrict this processing and they request we do so.

- **The right to data portability** – we provide customers with appropriate data in a format that allows it to be portable (i.e. usable by another landlord).

- **The right to object** – we ensure we stop processing ***personal data*** where the ***data subject*** requests this and they have a legal basis for doing so.

- Rights in relation to automated decision making and profiling – we do not make automated decisions that have a serious effect on the rights and freedoms of the ***data subject***.

Form of Request: The employee must complete the **GDPR Rectification of Data Request Form**. It asks the applicant to provide their name, contact details and evidence of identity, along with such other information to enable us to identify both you and the personal data that you are requesting be rectified.

Timescale for Compliance: An individual has the right to require Westfield Housing to rectify their personal data without undue delay, and in any event within one month of receipt of the request. However, if the request is complex or the individual has made numerous other requests, we may extend the time period for response by two further

months where necessary. If we need to exercise this limited right to extend, we must inform the individual within one month of receipt of their request, and we will also explain to them the reasons for the delay in responding.

Third Parties: An individual must communicate any rectification of personal data carried out in accordance with a request to each third-party recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. We will also inform the individual about those recipients if we are requested to do so.

7.2 We acknowledge that individuals have the right to expect we will have appropriate and reasonable safeguards and any third parties engaged by us to protect the confidentiality, integrity and security of all personal and sensitive personal information.

7.4 We will respond to Subject Access Requests within one month of receipt and when identification of the ***data subject*** has been verified (unless these are complex where we may respond in two months – but will inform the ***data subject*** of this as soon as practicable but within one month). Further information to be found in the Subject Access Request Procedure.

8. Sharing data with others

8.1 When a contract with a third party includes a requirement or need for them to process data on our behalf we will ensure they are able to meet the requirements of data protection legislation as part of the tender process. This will include how and where they process or store our ***personal data***

8.2 Where a third party acts as a ***data processor*** on our behalf we will ensure through a legal agreement that the third party also operates in accordance with the data protection legislation and associated legislation, regulation and codes of practice that the ICO publish. We will take appropriate action against the third party where they operate outside of any data sharing agreements or contractual terms.

8.3 We do not allow our ***data processors*** to use sub-processors without our approval. We will only give this approval where we are satisfied they are able to meet the requirements of the data protection legislation, including how and where they process or store our **personal data**.

9. Personal Data Security Breach Procedures

9.1 Where there is a ***personal data security breach*** this will be reported to the CEO and Chairman within 48 hours, and ICO if appropriate, identifying the cause, evaluate the impact and make a report. All breaches should be reported to the Board in due course.

9.2 We store data in several locations (including secure back-ups) with adequate security to ensure the rights of the ***data subject*** are upheld.

10. Related Procedures and Documents

10.1 Subject Access Request Procedure
10.2 Subject Access Request Log Book
10.3 Privacy Notices
10.4 Data Cleansing Forms
10.5 Confidentiality Agreements for Third Parties (Contractors)
10.7 Rectification of Data Request Form
10.6 NHF Document Retention Schedule
10.7 Westfield Housing Association Retention Schedule