# Red Kite Group

# Privacy and

# Data Protection Policy

| | | | |
|---|---|---|---|
| **Version:** | **6** | **Approved by:** | **Board** |
| **Effective Date:** | **18th July 2019** | **Approval date:** | **17th July 2019** |
| **Policy reviewer:** | **Group Governance Manager** | **Policy owner:** | **Data Protection Officer** |
| **Review period** | **3** | **Next review due by:** | **July 2022** |

Partnership • Respect • Pride • Creativity

Realising the potential in our communities

## 1. Purpose

1.1 This policy sets out the approach of Red Kite Group to protecting the privacy of ***data subjects*** (our customers, volunteers 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 Red Kite Group consists of:

- Red Kite Community Housing Limited
- Twenty11 (Homes) Limited
- Pennvale (Holdings) Limited
- Edenmead Limited
- Red Kite DevCo Limited

1.3 The implications of non-conformance with the data protection legislation to us as a business are three-fold

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

1.3.2 Intervention and fines (of up to 20m euros or 4% of annual turnover for serious breaches) by the Information Commissioner Office

1.3.3 Regulatory downgrade from the Regulator of Social Housing

1.4 This is one of a suite of data protection policies. Section 8 details the other policies.

## 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 what data is collected and what it is used for

**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 Regulations lists these as:

- Race
- Ethnic Origin
- Political Beliefs
- Religion
- Trade Union Membership
- Genetics
- Biometrics (Where used for ID purposes)
- Health
- Sex Life
- Sexual Orientation

**Personal Data Security Breach** – an incident that has affected the confidentiality, integrity or availability of personal data. This could be when personal data 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 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 This outlines the responsibilities for this policy (further responsibilities are laid out in the related data protection policies)

3.2 **Red Kite Board** – to approve this Group policy and to approve the annual data protection compliance report on our compliance with this (and other relevant policies) and receive reports where there have been Personal Data Security Breaches

3.3 **Chair of Audit and Risk Committee** – to receive reports on data security breaches where there is an obligation to report to the ***ICO*** prior to reporting to the ***ICO***

3.4 **Audit and Risk Committee** – to receive quarterly data protection compliance reports, recommend an annual compliance report to the Red Kite Board and to accept reports on Personal Data Security Breaches. To monitor the progress of data protection implementation plans

3.5 **Red Kite Chief Executive Officer** – overall responsibility for ensuring compliance with this policy (and other data protection policies)

3.6 **Data Protection Officer (DPO)** - The Red Kite Group has a voluntary DPO as we do not meet the threshold for requiring a mandatory DPO. The DPO role is the lead staff member for data protection. The DPO ensures our policies are up to date and being adhered to, our major projects have privacy by design built in, ensures staff and volunteers have appropriate training, ensures the rights of ***data subject*** are upheld and leads on ***Personal Data Security Breach*** investigations. This role is fulfilled by the Governance and Regulation Manager

3.7 **Head of Commercial** – ensuring contracts are compliant with data protection legislation

3.8 **Head of Progress** - ensuring that information security is maintained and meets the requirements of data protection laws and our data protection policies

3.9 **All staff and volunteers across the group structure** – ensuring they are compliant with our privacy and data protection policies

## 4. Legal Framework

4.1 There are three key pieces of data protection legislation

- ***General Data Protection Regulations (GDPR)*** – this comes/came into force on 25th May 2018 and replaces 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.

- ***Data Protection Act 2018***– the DPA 2018, covers the areas in the GDPR for member states to determine locally

- ***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, volunteers 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 we build *privacy by design* into new ways of working (e.g. a privacy impact assessment will be carried out for all projects to identify any privacy risks for the project to address)

5.6 We will ensure all staff, volunteers and Board/Committee members receive appropriate training for their role

5.7 We will ensure all personal data breaches are investigated and, where appropriate, report to the ***ICO*** within 72 hours. The Chair of the Audit and Risk Committee will also be notified of breaches that require reporting to the ICO prior to reporting.

## 6. Policy Statement

### *6.1 Accountability and Governance*

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

6.3 The Red Kite Board is ultimately responsible for compliance with the requirements of data protection legislation.

6.4 We have a voluntary Data Protection 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

6.5 We have a clear Privacy Notice for each subsidiary on their relevant website. 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)

6.6 **Personal Data Security Breaches** of this policy will be reported to Audit and Risk Committee

6.7 An annual Data Protection compliance report will be presented to Audit and Risk Committee

6.8 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. Personal data will be

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- personal data is accurate and, where necessary, kept up to date
- kept in a form which permits identification of ***data subjects*** for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data

***6.9 Rights of the data subject***

6.10 We ensure that we comply with the rights of the ***data subject***

- The right to be informed – we have a privacy notice that informs ***data subject*** 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 – we amend personal data where it is inaccurate of incomplete
- The right to erasure – we delete ***personal data*** when a ***data subjects*** 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***

6.11 We process ***Special Category Data*** and other sensitive data with greater protection and where relevant put appropriate safeguards in place to protect the privacy of the ***data subject***

6.12 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

6.13 We will respond to Subject Access Requests within one month of receipt and identification of the ***data subject*** (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).

6.14 ***Sharing data with others***

6.15 We only share data with a third party where we have a data sharing agreement in place, where we are required to by law or where we have the consent of the ***data subject*** (e.g. where a tenant gives another person authority to act on their behalf)

6.16 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***

6.17 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.

6.18 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**.

6.19 ***Personal Data Security Breach***

6.20 Where there is a ***personal data security breach*** we will comply with our Personal Data Security Breach Management Policy and related processes. This policy ensures we meet the requirements of the GDPR

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

6.22 We only transfer or store data within the EEA or with third parties in a country outside the EEA where they have adequate safeguards in place to enable the ***data subject*** to enforce their rights under the GDPR. If we are to transfer or store data outside of the EU this will be subject to appropriate information governance and security control checks and will need the approval of a member of EMT.

6.23 ***Personal Data Security Breach*** will be managed in tandem with our IT Security Breach Incident Management Policy

***6.24 Privacy by Design***

6.25 We build privacy into our ways of working. We carry out Privacy Impact Assessments before we make major changes to ensure any risks to privacy are identified and ways to mitigate these are delivered through a structured project plan.

## 7. References

7.1 ICO – Guide to the General Data Protection Requirements

7.2 ICO – Guide to the Privacy and Electronic Communications Requirements

7.3 ICO – Conducting Privacy Impact Assessments Code of Practice

7.4 ICO – Privacy Notices Code of Practice

7.5 Information and Privacy Commissioner of Ontario – Privacy by Design

## 8. Related Policies & Procedures

8.1 Personal Data Security Management Breach Policy

8.2 Personal Data Security Management Breach Process

8.3 CCTV Policies

8.4 Information Management and Security Policy

8.5 Information Security Incident Management Policy

8.6 Subject Access Request Process