Data Protection Policy

Version 5 | May 2016

Reference	**RS002**	**Version**	**5**
Issue date	**May 2016**	**Review date**	**May 2018**

Partnership • Respect • Pride
Excellent services for you and your community

1 Introduction and Scope

1.1 This policy relates to the Data Protection Act 1998 (Act) and to our (Red Kite Community Housing Limited) internal procedures for processing peoples' personal and sensitive personal information. This policy outlines our obligations and commitment to ensure that individuals' rights are upheld in relation to the confidential, personal and sensitive personal information that we hold and process.

1.2 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.

1.3 The Act requires us as a Data Controller to process personal information in accordance with the eight data protection principles in relation to the running of our business and delivering our services.

1.4 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.

1.5 Where a third party processes personal information on our behalf we will ensure through a legal agreement that the third party also operates in accordance with the Act and associated legislation, regulation and codes of practice that the Information Commissioner Office (ICO) publish.

1.6 We understand that the consequences of failing to comply with the requirements of the Act may result in:

- Personal accountability and liability
- Organisational accountability and liability
- Criminal and civil action
- Enforcement powers and fines being issued by ICO
- Loss of confidence in the integrity of our systems and procedures
- Significant reputational impact and damage
- Individuals obtaining compensation for damages in relation to data protection breaches
- Disciplinary action

1.7 This policy applies to data held either manually or within electronic systems that are deployed for the processing of personal and sensitive personal information. It outlines our and our affiliates' obligations and commitment to compliance with the DPA and also serves to ensure that people's rights are upheld.

1.8 The Act requires that we, as a data controller, process personal information in accordance with the eight Data Protection Principles which we have adopted. In relation to good information handling these principles are:

- Fair and lawful
- Specific to purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept for no longer than necessary
- Processed in accordance with data subjects rights
- Kept secure
- Not transferred overseas without suitable safeguards

2 Definitions

2.1 The Act is designed to ensure that we meet our obligations and ensure people who access our services and/or are applicants or prospective employees of Red Kite can exercise their rights in relation to the processing of their personal information. The Act defines that we are responsible for processing the personal information as the 'Data Controller', and people as individuals are 'data subjects' and that their personal information is defined as 'personal data'.

2.2 We will take all reasonable measures and actions to meet our obligations under the Act. We will ensure correct data processing requirements are in place to protect people's personal information where it is shared with third parties, (data processors) who are acting under our instruction to process our people's personal information on our behalf.

2.3 We will ensure personal and sensitive personal information is fairly and lawfully collected in line with peoples' rights. In doing so we will ensure Personal and Sensitive Personal information is collected, processed and shared in line with schedule 2 and 3 of the Act. We will abide by the law to ensure the confidentiality of our peoples' information and ensure any information sharing is not carried out with unauthorised third parties. When information sharing, we will consider any possible adverse effects on the individual(s).

3 Policy Statement

3.1 We will adopt and follow this policy and the requirements of the supporting Data Protection, Information Governance and Security Framework(s) and System(s). The core requirements relate to the:

> Collection, storage and processing of our records and the confidentiality and security of our peoples' information. The management recording and response to security incidents and how we retain and securely destroy our peoples' personal information when it is no longer required. We will ensure information is readably available in line with the Act and its exemptions and ensure the integrity of all the personal information we collect and process.

3.2 We will only collect and process personal and sensitive information that has been obtained fairly and lawfully and for a specific set of purposes or where we have legitimate purpose(s) under the law to do so. Personal Information will be adequate and relevant and only used for the purposes collected. It will be maintained and kept accurate with the help of the individual and not retained for any longer than is necessary.

3.3 We will ensure personal or sensitive personal data is processed in line with the law, kept both secure and confidential at all times and ensure all individuals governed by this policy will:

- Only access and process peoples' personal information that they are authorised to do on our behalf
- Adhere to all Information Governance, Data Protection, Security, Human Resources frameworks and procedures supporting this policy
- Only share information with third parties where it is fair and legal to do so and in accordance with published fair processing notices
- Apply the ICO good practice codes in Subject Access Request, Data Sharing, Privacy Impact Assessments and Employment Practice
- We will adopt the good practice set out by the ICO CCTV code of practice in all our operating systems

3.4 We will ensure all existing and new employees, board members and volunteers undertake data protection and security training and as part of this they will be accountable to embed and promote good information handling and security and apply the eight data protection principles. There will be an induction programme for new starters who will undertake an applicable course within three months of starting and refresh every 12 months or as and when the law requires.

3.5 We are committed to ensuring that all appropriate technical and organisational measures are taken to prevent against unlawful access, process, accidental loss or destruction of or damage to personal information we hold. We will operate a clear desk, work station and building access standard. We will ensure all fixed and mobile devices are kept secure and aim to ensure all mobile devices are encrypted and have restricted access to the use of memory sticks and that USB ports are managed in line with this and our security governance controls.

3.6 We will only transfer personal information to jurisdictions outside the European Economic Area (EEA) if it has a recognised and adequate level of protection for data protection purposes. Transferring data outside of the United Kingdom requires a director's approval and with relevant Information Governance and Security compliance checks.

3.7 The directors and Senior Management Team are responsible for reviewing the annual notification and ensuring their business areas report changes or new forms of processing to the Data Protection Officer who will make the necessary arrangements to notify the Information Commissioner Office (ICO). An annual compliance report will be presented to Audit and Risk Committee which will include our annual notifications.

3.8 We will comply with all relevant data protection processing, privacy notices and notifications to any future acquisition and/or merger with third parties, including for example our obligations under Transfer Undertakings Protection of Employment Regulations. We will ensure that all personal or sensitive personal information is only shared where legally required and anonymised as part of any testing, evaluation of assets and liability assessments except as required by law.

3.9 We will ensure that all individuals from whom we collect and process personal information are made aware via privacy statements/notices etc. of the identity of the data controller and data processor and the reasons why personal and sensitive personal data is required to be processed by the respective parties and how their information will be processed, securely stored, or disposed of and when we need their consent to collect and share this information.

3.10 We acknowledge that individuals have further rights. Full rights detailed in our *Accessing Your Information Leaflet including*:

- To make a request in writing for access to and be provided with a copy of their personal data that they are entitled to receive under the Act. We will apply a £10 fee as defined in the Act and respond to requests within 40 calendar days upon receipt of a formal and valid request;

- To request that their personal data is deleted or corrected if they believe the information is inaccurate, excessive or out of date. We will comply with the applicable requirements of the Act and respond within 21 calendar days of receiving the request

- To prevent the processing of their data (if it is as defined in the Act), causing damage or distress to them, in relation to automated decision-making and to opt-out of processing for direct marketing purposes

- Disclosure of personal and sensitive personal data shall be assessed in line with the exemptions of disclosure as defined in the Act. Individual or third party data will be deemed confidential and will only be disclosed or shared with the consent of the individual and/or where we are legally obliged to under the Law

3.11 We will ensure that all our people are made aware of our approach and obligations in respect of the Act and associated legislation and regulation.

3.12 Complaints relating to alleged breaches of the Act or complaints that an individual's personal information is not being correctly processed will be assessed and responded to by the Data Protection Officer. All complaints of alleged customer service dissatisfaction will be separately processed in accordance with our complaints procedure only after the Data Protection Complaint has been fully reviewed and responded to.

3.13 We will consider taking internal disciplinary or contractual/legal action where individuals governed by this policy do not comply with this policy, the Act and our associated frameworks, policies and procedures.

4 Information Sharing

4.1 We will only share personal information in accordance with the eight Principles of the Act and as required by law or regulation. We will only share relevant information with partners and selected third parties who are working on our behalf, or with whom we have a legitimate interest to share individuals' personal information. We will inform individuals how we will process and share their personal information via our privacy policies and fair processing notices. Examples and purposes for sharing information are:

- For the prevention or detection of crime and apprehension or prosecution of offenders
- For the assessment or collection of tax or duty owed to customs and excise, which may include utilities' where a customer owes a debt

- When required in connection with legal proceedings or gaining legal advice
- In relation to the physical or mental health of an individual to protect their and others' interests
- For research purposes
- To comply with the law
- Where it is in our legitimate interests or as part of our legal or regulatory obligations we may receive and share individual personal data. In doing so we will consider if the sharing may prejudice the rights and freedoms or interests of the individual and act accordingly and within the law

5 Marketing and Promotion of Goods and Services

5.1 We will NOT share or sell your personal data to other third-party organisations for the purposes of marketing or promotion of goods and services. We may contact you with information about our services which are relevant, similar or complement existing services which you already receive from us. If you do not wish to receive these offers you should contact our Relationship Team.

6 Confidentiality

6 All current and former employees, board members, volunteers, suppliers and contractors are responsible and accountable for security and confidentially of company and individuals data that they process. A breach of this and policies below will be deemed a serious offence. Any person(s) found to share/disclose or obtain data without consent and found to have knowingly, recklessly, deliberately or without authorisation breached these instructions or policies renders him/herself liable for disciplinary, contractual and/or legal prosecution in accordance with our Employment and/or Supplier/ Contractor obligations including:

- NHF Governance Code
- Disciplinary Policy
- Employment Contracts and Code of Conduct (confidentiality clauses)
- Information Security Policy

7 Equality and Diversity

7.1 We will ensure that this policy is applied fairly and consistently. We will not directly or indirectly discriminate against any person or group of people because of their race, religion / faith, gender, disability, age, sexual orientation, gender reassignment, marriage and civil partnerships, pregnancy and maternity or any other grounds set out in the Equality Act.

8 Responsibilities

8.1 The Head of Finance has delegated responsibility for ensuring we meet our obligations in relation to Data Protection. The Head of Finance will also be responsible for the annual registration with the Information Commissioners Office.

8.2 We will ensure that there is always a named Data Protection Officer who will act as a main contact point for any queries in relation to Data Protection. This role will be undertaken by the Governance and Regulation Manager.

8.3 All staff, Board Members and Volunteers have a responsibility to ensure that they comply with the Policy, ensuring any relevant parties whom they work with, are also aware of their obligations.

9 Review

9.1 We will carry out an annual health check taking account of legislative and regulatory changes and a fundamental review of this policy every two years.