Sparrow
Shared Ownership

Data Protection Policy

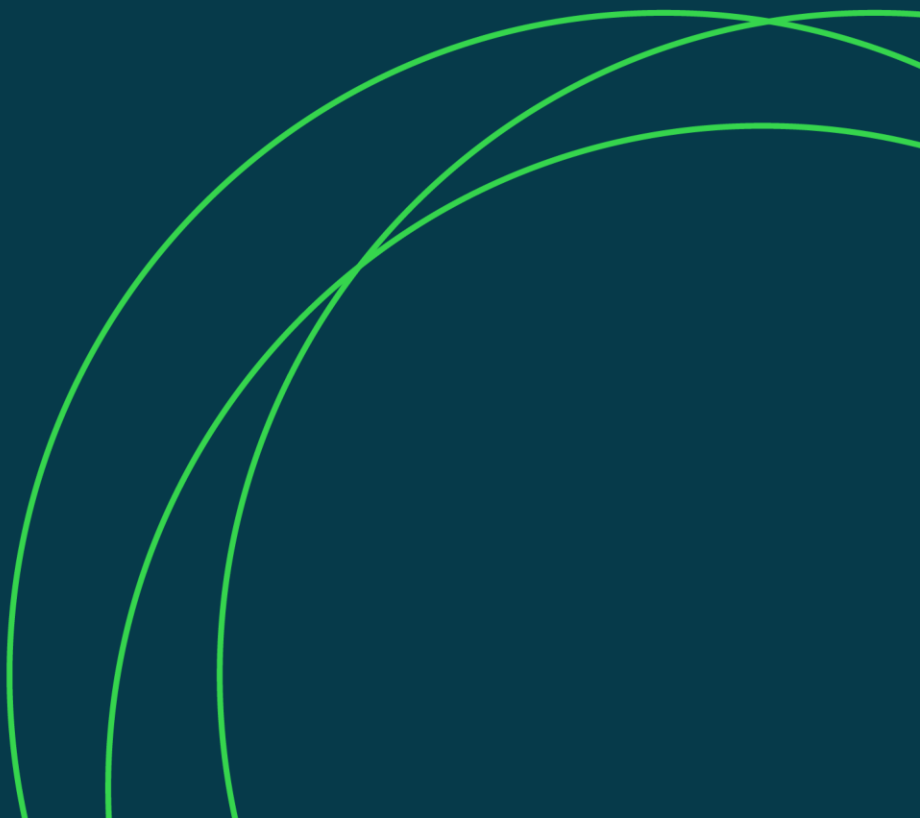
CODE:

VERSION: [1.0]

CREATED: [07/11/2024]

REVIEW: [07/11/2025]

AUTHOR(S): [Data Protection Officer]



Data Protection Policy

1. Our policy statement

1.1 To operate, Sparrow Shared Ownership Limited (Sparrow) must collect and use information about people - primarily our customers but also prospective customers, employees, contractors, and other third parties.

1.2 Additionally, Sparrow may be required by law to collect and use information to comply with its contractual obligations and its legislative and regulatory requirements.

1.3 The use of personal information is subject to a complex array of data protection laws. Personal information (definition set out in Appendix A) must be handled and dealt with properly, no matter how it is collected, recorded, and used, and whether it is on paper, in computer records or recorded by other means such as CCTV.

1.4 The objective of this policy is to ensure that:

1.4.1 Sparrow's staff are aware of the requirements of data protection law and guidance and how Sparrow deals with personal data, and know what to do and when to seek advice; and

1.4.2 as a result, Sparrow complies with applicable data protection laws and guidance and discharges all of its legal obligations in this respect.

1.5 For the definition of certain terms used in this policy please refer to Appendix A (Data Protection Definitions).

2. The scope of this policy

2.1 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present staff, customers, suppliers, or any other Data Subject.

2.2 This Data Protection Policy applies to all Sparrow's personnel - including employees, workers volunteers, directors, consultants and contractors ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on Sparrow's behalf and attend training on its requirements.

2.3 The correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that Sparrow must take seriously at all times.

2.4 In the event of a failure to comply with data protection law, Sparrow may be exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher, depending on the breach.

2.5 Data protection is the responsibility of everyone within Sparrow, and this Data Protection Policy sets out what Sparrow expects from you when handling Personal Data to enable the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Procedures are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related

Policies and Procedures. Any breach of this Data Protection Policy or its associated Procedures may result in disciplinary action.

2.6 Directors and Heads of Service are responsible for ensuring that all employees follow the policy and support the accuracy, completeness, and integrity of all records that their team is responsible for and encourage good information security.

3. The Data Protection Officer

3.1 Sparrow's Data Protection Officer (DPO) is responsible for overseeing this policy and, as applicable, developing Related Policies and Privacy Guidelines.

3.2 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

3.2.1 if you receive a Data Subject Access Request (DSAR) or need any assistance or advice on any question asked by a Data Subject relating to their data protection rights;

3.2.2 if there has been a Personal Data Breach;

3.2.3 if you need to Process Personal Data on Sparrow's behalf and you are unsure whether or not we are lawfully able to do so; or

3.2.4 if you are unsure what security or other measures you need to implement to protect Personal Data.

4. Principles and lawfulness

4.1 There are six legal 'data protection principles' that underpin the Processing of Personal Data. We have listed these principles in Appendix B.

4.2 Under the law, every individual or data subject has certain rights in respect of the personal information Sparrow holds on them. We have listed these data subject rights in Appendix B.

4.3 Sparrow has developed procedures to ensure that its day-to-day operations are conducted in accordance with the law and the principles and data subject rights summarised above. Our approach is set out below and further detailed in the Related Policies and Procedures. If you are going to carry out any new Processing or any Processing that does not seem to be covered by our Procedures, please contact the data protection team for advice or further information.

5. Our approach

Data Security

5.1 For data security purposes staff working from home must not send customer or confidential information to their home email address, anyone found doing so maybe subject to disciplinary action. You are advised to lock your screen before moving away from your desk.

5.2 Paper files containing personal information must be stored in lockable cabinets. When in use, confidentiality of the file must not be compromised. Files must not be left lying open

where other people can see them. Files must not be left out overnight or left unattended on desks but locked away in a secure location.

5.3 Where customer information needs to be taken from a Sparrow Office, staff must take particular care. If travelling by car, information must not be left where it is visible but ideally locked in the boot. At night information must be securely locked in an office or the staff member's home. Customer information must not be left in a car overnight.

5.4 Staff using memory sticks and laptops will be responsible for keeping them secure at all times.

Data Sharing

5.5 Sparrow will most commonly share the personal data it collects with its contractors, who deliver housing management services with us. Personal information is also shared with Local Authority partners when providing housing to referrals from their local housing lists.

5.6 In some circumstances, it may be appropriate to disclose information held by Sparrow to specific third parties for example to prevent a criminal offence from being committed, or to prevent the continuation of a criminal offence. We must enter into data sharing agreements with contractors and specific third parties before sharing personal data and confidential information with them to ensure that Sparrow and its customers are protected.

Data Retention

5.7 Personal data must only be kept for the length of time necessary to perform the process for which it was collected. This applies to both electronic and non-electronic data.

5.8 Individuals can request deletion of certain types of information about them deleted where one of a number of circumstances apply (the right to be forgotten). Should an individual contact you with a request to delete their personal data, please either direct them to email, or forward their request to the Data Protection Officer (DPO)

5.9 Where personal and confidential information is no longer required, it will be destroyed. Please consult the Data Retention Policy for further information.

Data Protection Impact Assessments (DPIA)

5.10 Before Sparrow undertakes any new Processing activity, it must consider whether a DPIA is needed. Sparrow will conduct a DPIA if the new Processing activity is likely to result in a high risk to the rights and freedoms of natural persons.

5.11 Directors and Heads of Service must ensure a DPIA is carried out when proposing a major system or business change programme, or conducting reviews of such programmes which involve:

5.11.1 the use of new technologies or changing technologies (programs, systems or processes);

5.11.2 automated processing including profiling and automated decision making;

5.11.3 large scale processing of special category personal data or other sensitive data such as criminal offence data;

5.11.4 large scale systematic monitoring of a publicly accessible area.

5.12 Any deployment of audio recording, video recording, CCTV or other monitoring and surveillance technologies will be in compliance with legal obligations and may need to involve the use of a DPIA.

5.13 The record of the DPIA must be filed with the Data Protection Officer.

Automated processing and decision making

5.14 Generally, Sparrow does not engage in automated processing/profiling, or automated decision-making. Some business services are supported by rule-based logic for the benefit and convenience of its registrants, for instance web-based registration automatic renewal systems that its registrants can use.

5.15 If/where Sparrow does ever engage in automated decision making/profiling, Sparrow will take steps to inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision. Where possible, Sparrow will do this prior to the decision being taken.

5.16 A DPIA must be carried out before any Automated Processing (including profiling) or Automated Decision-Making activities are undertaken.

Privacy by Design

5.17 Sparrow will implement appropriate technical and organisational measures like pseudonymisation of personal data, in an effective manner, to ensure compliance with data privacy by design principles.

5.18 Managers are responsible for assessing what privacy by design measures can be implemented on all programmes, systems and processes that process Personal Data by taking into account the cost of implementation; the nature, scope, context and purposes of processing; and the risks of varying likelihood and severity for individuals' rights and freedoms posed by the Processing.

Privacy Notices

5.19 When personal data is collected from individuals, staff and others who process personal data on behalf of Sparrow, must ensure that the individual is made aware

- 5.19.1 who Sparrow is;
- 5.19.2 why we need to collect their personal information;
- 5.19.3 what we intend to do with the information;
- 5.19.4 who we may share it with or disclose it to (ie which types of organisations).

5.20 The 'How we use your information' privacy notice should be signposted to customers when personal information is first collected. This notice will be reviewed annually to ensure it reflects any changes in the way we Process Personal Data.

6. Equality and diversity

6.1 Sparrow is committed to making sure all services are accessible to all our customers. Our staff will be trained to make sure they are communicating appropriately with our customers, and they have the relevant information.

6.2 This policy will be applied in a way which makes sure we treat all customers with fairness and respect. We recognise our duty to advance equality of opportunity and prevent discrimination or victimisation on the grounds of age, sex, sexual orientation, disability, race, religion or belief, gender re-assignment, pregnancy and maternity, marriage and civil partnership and any other protected characteristic defined within the Equality Act 2010.

6.3 On request we will provide translations of all our documents, policies and procedures in various languages and formats including braille and large print.

7. Delivery of this policy

7.1 This policy should be read alongside the following:

7.1.1 All Sparrow Information Security Policies and Procedures

7.1.2 CCTV and Doorbell Camera Policy

VERSION	CHECKED BY	AMENDMENTS	APPROVED AT/BY	DATE OF APPROVAL	PUBLISHED BY	DATE OF REVIEW
1.0	Jamie Flintoff		Board	07/11/2024	Nadine Ofori-Atta	07/11/25

Appendix A

Definitions

UK GDPR contains a number of terms used in this policy and the definitions are set out below:

- Personal data - is any information relating to a living individual who can be identified:
    - from that information,
    - or from the information and other information in the possession of, or which may come into the possession of, the data controller.

It includes opinions about an individual and indications of the intentions of any person towards that individual.

- Processing - is what is done with information or data. It includes how information is obtained, recorded, held, organised, altered, disclosed, transmitted, combined with other information, and destroyed.
- Data controller - means the organisation which collects/holds the data and which is responsible for determining the purpose and manner in which personal data is processed. The data controller is responsible for compliance with the DPA but may not always be the organisation which processes that data.
- Data subject - is the living individual who is the focus of or described by the personal data.
- Data processor - is a third party engaged to process data on behalf of the data controller. If the data controller uses a data processor it must comply with specific provisions in the DPA.
- Sensitive personal data - means data given special status under the DPA:
    - the racial or ethnic origin of the data subject,
    - their political opinions,
    - their religious beliefs or beliefs of a similar nature,
    - any trade union membership,
    - their physical or mental health or condition,
    - their sexual orientation, or other aspects of their sex life.
    - the commission or alleged commission by them of any offence, and
    - any proceedings for any offence committed or alleged to have been committed, the outcome of those proceedings, including the sentence of any court.

Sparrow
Shared Ownership

Appendix B

GDPR: Legal principles

Personal data must:

1. Be processed fairly, lawfully and transparently (Fairness, lawfulness and transparency);
2. Be collected and processed only for specified, explicit and legitimate purposes (Purpose limitation);
3. Be adequate, relevant and limited to what is necessary for the purposes for which it is processed (Data minimisation);
4. Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay, once it becomes clear it is inaccurate (Accuracy);
5. Not be kept for longer than is necessary for the purposes for which it is processed (Storage limitation);
6. Be processed securely. To that end the Council adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, distribution or damage (Integrity and confidentiality).

In addition, there is an overarching principle of accountability: Sparrow is responsible for complying with the UK GDPR and being able to demonstrate this. (Accountability).

Personal Data can only be lawfully processed if one or more of the following conditions apply:

1. The data subject has given consent to the processing;
2. Processing is necessary for the performance of a contract with the data subject;
3. Processing is necessary for compliance with a legal obligation to which the data controller is subject;
4. Processing is necessary to protect the vital interests of the data subject or another person;
5. Processing is necessary for the performance of a task carried out in the public interest;
6. Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

Separate conditions must apply if special category data or criminal records data is to be lawfully processed.

GDPR: Data subject's rights

Data Subjects have the following rights in respect of their personal data:

- The right to be informed
- The right to erase

- The right of access
- The right to restrict processing
- The right of rectification
- The right to data portability
- Rights in relation to automated decision making and profiling
- The right to object