CAMFIELD CRAWLEY

Giving people room to create a better future.

Data protection policy

April 2024

CRAWLEY FRIENDS HOUSING ASSOCIATION LTD.

DATA PROTECTION POLICY

1. Introduction

1.1 Crawley Friends Housing Association (CFHA) understands the importance of protecting the data of its residents, staff, trustees and visitors. This policy outlines how CFHA will govern the processing of personal data and its compliance with data protection legislation.

1.2 The Data Protection Act 2018 (DPA) sits alongside The UK General Data Protection Regulation (GDPR UK). It applies to personal data (being data that allows any living individual to be identified) that is:

(a) Held on a computer or any other automated system (including e-mails, documents, data on mobile phones, iPads etc.).

(b) Held in a relevant filing system (either paper or electronic) that is organised alphabetically by the name of the person or some other identifier.

(c) Intended to go onto computer or into a relevant filing system.

1.3 According to the Information Commissioner's Office, Personal data will be protected under the regulations if it is information that is:

(a) Being processed by means of equipment operating automatically in response to instructions given for that purpose.

(b) Recorded with the intention that it should be processed by means of such equipment.

(c) Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

(d) Recorded information held by a public authority.

(e) Held on computer or is intended to be held on computer.

2. Aims and objectives

2.1 The purpose of this policy is to enable Crawley Friends Housing Association to:

- Comply with the General Data Protection Regulation (GDPR) in respect of the personal data it uses
- Follow good data management practice.
- Protect CFHA's residents, staff, and partners through commitment to privacy protection.
- Reduce the risk of breaching Data Protection compliance requirements.
- Protect the organisation from the consequences of a breach of Data Protection compliance.

3. Definitions

3.1 **"Data"**: Information that is a) processed by means of equipment operating automatically in response to instructions given for that purpose, b) recorded with the intention that it should be processed by means of such equipment, c) recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

3.2 **"Data subject":** An individual who is the subject of **personal data**. Data subjects have legal rights in relation to the handling and processing of their personal data.

3.3 **"Personal data":** Any data which relates to an individual who can be identified a) from that data or b) from that data and other information in - or likely to come into - CFHA's possession. Personal data can be factual (e.g. name, address, or date of birth) or an opinion (e.g. performance appraisal).

3.4 **"Data Controller":** A person who (either alone or jointly with other persons) determines the purposes for which, and the manner in which, any **personal data** is to be processed. They have a responsibility to establish practices and policies in line with the appropriate data protection legislation.

3.5 **"Data users":** employees whose work involves the use and/or processing of **personal data**. Data users have a duty to protect the information they handle by following and adhering to the Data Protection and Information Security policies at all times.

3.6 **"Data processors"**: Any person, other than an employee of the Data Controller, who processes **personal data** on behalf of a Data Controller, i.e. third parties that process or handle personal data on CFHA's behalf.

3.7 **"Processing"**: Any activity that involves use of **personal data**. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasure or destruction. Processing also includes transferring personal data to third parties.

3.8 **"Sensitive personal data"**: Includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. **Sensitive personal data** can only be processed under strict conditions, and usually requires the express consent of the **data subject**.

3.9.1 **"Relevant filing system"**: Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

3.9.2 It is intended to cover non-automated records that are structured in a way which allows ready access to information about individuals. As a broad rule, a **relevant filing system** exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals.

3.10 **"Data Protection Legislation"**: refers to the Data Protection Act 2018 and the UK GDPR.

4. Policy Statement

4.1 The scope of this policy applies to all employees, trustees and any third party or individual, who conducts work on behalf of CFHA. This policy requires compliance with the appropriate data protection legislation in relation to all personal data (including Sensitive Personal Data) that CFHA happens to process.

4.2 CFHA will ensure compliance to protecting personal data by:

(a) complying with both the law and good practice;

(b) respecting an individual's rights;

(c) being open and transparent with an individual whose data is held;

(d) providing training and support for staff who handle personal data (if required);

(e) ensuring that sufficient resources are available so that the provisions of data protection legislation can be met;

(f) ensuring that policies and procedures that involve the processing of personal data support compliance with data protection legislation;

(g) keeping information securely in the right hands;

(h) holding good quality information.

5. Safeguarding Individuals

5.1 The organisation recognises that its priority under the appropriate data protection legislation is to avoid causing harm to individuals. CFHA therefore commits to keeping information securely in the right hands and holding good quality information.

5.2 This policy aims to address the following risks related to the use of personal data:

(a) Breach of confidentiality (information being given out inappropriately).

(b) Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed.

(c) Breach of security through unauthorised access, theft, or loss of computer equipment.

(d) Failure to establish efficient systems of managing changes to data, leading to personal data being not up to date.

(e) Harm to individuals if personal data is not up to date.

(f) Data Processor contracts being unclear about their responsibilities.

(g) Data not being properly identified and catalogued.

6. Data Protection Principles

6.1 All processing of personal data must be done in accordance with the following data protection principles, and CFHA's policies and procedures are designed to ensure compliance with them. There are six principles that cover issues including the processing, accuracy, security, and lawfulness of data collection as well as the rights of the Data Subject as follows:

(a) Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

(b) Data must be adequate, relevant, and limited to what is necessary.

(c) Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes (subject to exceptions).

(d) Data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to remove inaccurate information.

(e) Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

(f) Data must be processed in a manner than ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.

7. Transparency

7.1 CFHA will ensure transparency, with easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information will be communicated to Data Subjects in an intelligible form using clear and plain language.

8. Fair and Lawful Processing

8.1 CFHA is committed to ensuring that the processing of personal data in its organisation is done fairly and without adversely affecting the rights of the data subject.

8.2 CFHA will endeavour to inform the data subjects of the purpose for which the data is to be processed and any sharing with third parties to whom the personal data may be disclosed or transferred.

8.3 Personal data may only be processed for the specific purpose notified to the data subject when it was first collected, or for purposes specifically permitted by Data Protection legislation. Personal data must not be collected for one purpose and subsequently used for another. If it becomes necessary to change the purpose for which the data is being processed, the data subject must be informed of the new purpose before any processing occurs.

8.4 The trustees will ensure that procedures are developed throughout the organisation as appropriate to ensure that Individuals who supply CFHA with personal data are provided with a 'Privacy or Fair Processing Notice' which communicates the following:

(a) The identity of the organisation.

(b) The purpose(s) for which personal data will be processed.

(c) Information regarding the disclosure of personal data to third parties.

(d) Information regarding the individual's right of access to personal data.

(e) Whether personal data is transferred outside the UK.

(f) How to contact CFHA with questions or queries regarding the processing of personal data.

(g) Details of specific technologies or electronic measures to collect information about individuals, e.g. website cookies.

9. Processing of Special Categories of Data and Data related to Criminal Convictions

9.1 Where CFHA undertakes the processing of personal data relating to criminal convictions and offences, it will only do so with a lawful basis and ensure transparency. Should consent be required, the organisation will ensure consent is obtained in an appropriate manner and explicit in alignment with the appropriate data protection legislation.

9.2 Where special categories of data are processed, the organisation will only undertake such processing with a valid lawful basis and special conditions. If consent is applicable, CFHA will ensure that it is able to be evidenced and obtained in alignment with the data protection legislation.

9.3 CFHA will ensure the necessary security measures and safeguards are in place when undertaking such processing.

10. Data Subject Rights

10.1 CFHA will ensure that the rights of data subjects are respected, and that they are able to exercise their rights. CFHA will ensure that a process for Subject Access Requests (SARs) is created and communicated so that staff can recognise requests, advise the subject on the correct process to be followed, and ensure the request is processed within the legal requirement of one month. CFHA will also ensure that:

(a) Data subjects can make subject access requests regarding the nature of information held and to whom it has been disclosed.

(b) They gain consent, where applicable, for sharing and dissemination of personal data for processing with partners.

(c) They prevent processing likely to cause damage or distress.

(d) They prevent processing for purposes of direct marketing.

(e) Data subjects are informed about the mechanics of any automated decision-taking process that will significantly affect them.

(f) Data subjects will not have significant decisions that will affect them taken solely by automated process.

(g) Data subjects can sue for compensation if they suffer damage by any contravention of the data protection legislation.

(h) Data subjects can take action to rectify, block, erase (including the right to be forgotten) or destroy inaccurate data.

(i) Data subjects can request the Information Commissioner's Office to assess whether any provision of the Data Protection legislation has been contravened.

(j) Data subjects have the right for personal data to be provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller.

(k) Data subjects have the right to object to any automated profiling without consent.

11. Review and Communication

11.1 The Trustees will ensure that, on a biannual basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive. On at least an annual basis, the Manager will review all the personal data maintained by CFHA by reference to the Records of Processing and Information Asset Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed. The Trustees will also:

(a) Ensure that all staff receive training in their responsibilities under Data Protection

(b) Ensure that all staff receive annual 'refresher' training, including modules on Data Protection.

(c) Disseminate Data Protection related guidance documents to staff to ensure that they conduct their duties in compliance with the legislation.

12. Transferring of Personal Data outside of the UK

12.1 CFHA will ensure that its processing does not result in personal data being transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data as permitted by appropriate data protection legislation.

13. Accountability

13.1 CFHA will adhere to the principle of accountability and ensure the organisation takes responsibility for ensuring compliance and equally for demonstrating that each processing operation complies with the requirements of the Data Protection legislation.

14. Records of Processing and Impact Assessments

14.1 CFHA will maintain the necessary documentation of all processing activities relating to personal data, and implement appropriate security measures, including performing a Data Protection Impact Assessment (DPIA) where there may be a high risk to the individuals concerned. A review of the records will be carried out every 12 months or whenever there is a substantial change to the processing activities, whichever is sooner.

15. Information Sharing Agreements

15.1 Where CFHA shares personal data with any third party, a 'Data Processor or Joint Controller Agreement' will be included as part of a formally documented written agreement or contract.

15.2 Where the other party uses the personal data for its own purposes, the agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information. When sharing, no personal data is to be shared without establishing:

(a) The legality and fairness of the purpose.

(b) The limiting of information disclosure in accordance with the purpose.

(c) The inclusion or exclusion of third-party information.

(d) The processing requirements throughout the information's lifecycle (including transfer, storage, and onward processing).

16. Sharing data under a legal obligation

16.1 Where the processing of personal data with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, are in compliance with the relevant law requiring disclosure of personal data, and are regularly reviewed and verified.

17. Accountability for Subject Access Requests

17.1 Although personal data may be processed by third parties, the responsibility for complying with a Subject Access Request will lie with CFHA where CFHA is the Data Controller or a joint controller.

17.2 Due to the requirement to provide the information needed in a request within one month, CFHA's contracts with third party processors must ensure there are arrangements to guarantee that Subject Access Requests are able to be dealt with promptly.

17.3 CFHA will ensure that its partners, suppliers, and stakeholders comply with Data Protection principles and information management in accordance with this policy, throughout the supply chain.

18. Complaints and data protection incidents

18.1 Data subjects who wish to complain to CFHA about how their personal information has been processed may lodge their complaint directly with the Trustees. Data subjects may also complain directly to the supervisory authority, which is the Information Commissioner's Office. Where data subjects wish to complain about how their complaint has been handled internally, or appeal against any decision made following a complaint, they may lodge a complaint to the Information Commissioner's Office.

18.2 Only the Chair of Trustees or the Company Secretary or an authorised delegate should communicate any personal data breaches to the Information Commissioner's Office on behalf of CFHA.

18.3 Where a data protection incident has been raised or identified, all employees and any third party or individual, who conducts work on behalf of CFHA must report this to the Trustees, who will acknowledge complaints and confirm appropriate actions. Unless formally directed by the Trustees in writing, employees should not provide formal responses to the outcome of any reported data protection incidents.

19. Retention and disposal of data

19.1 Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). CFHA's data retention and data disposal policy and procedures will apply in all cases. Appropriate measures are to be applied to protect the privacy and confidentiality of all personal data throughout its period of retention within the organisation. Staff must ensure that appropriate processes and procedures are applied to ensure the regular backup of data, and that backups can be restored when required, irrespective of the period for which they have been retained.

19.2 CFHA is committed to ensuring personal data are not retained for longer than it is required. Some data will be kept for longer periods than others, but all decisions are to be based upon operating requirements. A separate Records Management and Retention Policy exists and provides further guidance as to the retention periods and processes adopted by Crawley Friends Housing Association.

20. Data Security

20.1 As required by the Data Protection Principles, CFHA will implement appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and the accidental loss, or destruction, of or damage to that personal data.

20.2 The measures align with the basic information security principles of:

(a) Confidentiality – only those persons specifically authorised can access and/or use the data.

(b) Integrity – the data shall be accurate and relied upon for the purpose for which it is being processed.

(c) Availability –the data will only be provided to authorised persons upon receipt of a validated request.

20.3 Everyone with access to personal data pertaining to other employees, residents or trustees is to ensure that:

(a) The personal data which they hold, or process is kept securely.

(b) Personal data is not disclosed orally, in writing or in any electronic form to any unauthorised person, either deliberately or accidentally.

20.4 Requests for information must be specific, and the level of checks conducted may depend on the possible harm and distress which inappropriate disclosure of the information could cause to the individual concerned.

21. Roles and Responsibilities

21.1 It is a condition of employment that all employees, contracted third parties and individuals abide by the policies endorsed by CFHA.

21.2 Any person, who considers that this policy has not been followed in respect of personal data relating to themselves, or others, is to raise the matter directly with their line manager, or, if the matter cannot be resolved, with one of the Trustees.

21.3 Third party suppliers that store or process personal data on behalf of the organisation are designated Data Processors and shall be bound by a Data Processor Agreement.

22. The role of the Data Protection Officer

22.1 Under the UK GDPR, a company **must** appoint a DPO if at least one of the following applies:

(a) It is a public authority or body.

(b) Its core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking).

(c) Its core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

22.2 Organisations may voluntarily appoint a Data Protection Officer, even if the above circumstances are not applicable.

22.3 CFHA is currently of the opinion that its obligations under the UK GDPR can currently be discharged by its existing staff, supplemented by monitoring from the Trustees. This position will be re-appraised on a regular basis as part of the annual review of this policy.

23. Complying with this policy

23.1 **Monitoring compliance** - The Trustees will verify compliance with this policy through various methods, including but not limited to internal and external audits, and general feedback about operating procedures.

23.2 **Exceptions** - Any exception to the policy must be raised with the Trustees and approved by them in advance of exceptions taking place.

23.3 **Violations/Non-Compliance** - Unauthorised disclosure of personal data could result in a disciplinary matter that may be considered as gross misconduct.

24. Related documents

24.1 Other Crawley Friends Housing Association policies that may be used to help ensure effective Data Protection Management include:

- Record Management and Retention Policy
- Subject Access Request Procedure

25. Legislation and Regulations

25.1 The legislation listed in this policy is not intended to cover all legislation applicable to this policy. To meet the required Regulator of Social Housing's Governance & Financial Viability Standard outcome on adherence to all relevant law, CFHA will take reasonable measures to ensure compliance with any and all applicable legislation by reviewing policies and procedures and amending them as appropriate. The legislation listed within this policy was considered at the time of the development of this policy, but subsequent primary and secondary legislation, case law and regulatory or other requirements will be considered and the policy reviewed and adopted in accordance with the requirements set out therein, even should such subsequent legislation not be explicitly listed within this policy.

26. Review

26.1 This policy will be reviewed each financial year or sooner if there is:

- A significant incident relating to this policy
- An organisational change related to this policy
- A change in legislation