CHARING CROSS
HOUSING ASSOCIATION

PRIVACY POLICY

Date approved	**30 May 2018**
Review frequency	**Every three years**
Date of next review	**May 2021**

Privacy Policy

1.0 INTRODUCTION

The General Data Protection Regulations replaces the Data Protection Act 1998 and introduces a number of changes the way organisations such as Charing Cross Housing Association processes and manages the personal data it collects.

To effectively conduct its business, the Association requires to collect and use certain information about individuals, including tenants, factored owners, employees and other individuals the Association has a relationship with. As a result the Association holds a significant amount of data from a variety of sources. Much of this data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

Charing Cross Housing Association is committed to ensuring that the data it holds in relation to customers, staff and other individuals is managed in a secure and safe way.

The Privacy Policy sets out the Association's duties in processing personal data and outlines the procedures for managing it.

2.0 LEGISLATION

The Association will, at all times, comply with legislation relevant to the collection, handling and storage of personal information including:

- The General Data Protection Regulation (EU) 2016/679
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
- Any legislation that, in respect of the United Kingdom, replaces or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union

3.0 DEFINITIONS

Personal Data – that from which a living individual can be identified either by that data alone or in conjunction with other data held by the Association

Special Category Personal Data or **Sensitive** Personal **Data** – data that is sensitive in nature as it relates to reveals details about a data subject such as the individual's racial or ethnic origin, religious beliefs, political opinions, sexual orientation or heath

Fair Processing Notice – sets out the Personal Data processed by the Association and the basis for that Processing

Data Processor – is a third party that processes personal data on behalf of the Association

Data Officer – individual with has the over-arching responsibility to ensure the Association complies with Data Protection laws

Privacy Impact Assessments (PIAs) – a means of assisting the Association in identifying and reducing the risks that activities or operations have on the personal privacy of Data Subjects

4.0 DATA

The Association holds a variety of data relating to individuals such as tenants, owners and staff (also referred to as Data Subjects) which is known as Personal Data.

The Personal data held and processed by the Association is detailed within its Fair Processing Notice (Appendix 1) and the Data Protection Addendum of the Terms and Condition of Employment.

5.0 PROCESSING PERSONAL DATA

Under the GDPR the Association can process Personal Data on behalf of data subjects provided it is doing so on one of the permitted grounds which are;

- Processing with the consent of the data subject
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject
- Processing is necessary for the Association's compliance with a legal obligation
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Association's official authority
- Processing is necessary for the purposes of legitimate interests

6.0 FAIR PROCESSING NOTICE (FPN)

The Association is required to provide all customers whose Personal Data it holds with a Fair Processing Notice. Customers will be advised of the terms of the FPN and the notice issued from the outset of processing their Personal Data.

7.0 EMPLOYEES' DATA

The Association holds and processes Employee personal Data and, where applicable, Special Category Personal data or Sensitive Personal Data.

Details of the data held and how it is processed is contained within the Employee Fair Processing Notice which is provided to Employees along with their Contract of Employment.

A copy of any employee's Personal Data held by the Association is available upon written request by the employee submitted to the Director.

8.0 CONSENT

Good practice states that the use of Consent as the ground for processing Personal Data should only be used where no other alternative ground for processing is available. However there may be occasions where the Association is required to use this ground and is required to obtain consent to process a Data Subject's Personal Data.

In those circumstances Consent must be;

- In writing from the Data Subject
- Freely given

- For a specific and defined purpose (i.e. general consent cannot be sought)

9.0 SPECIAL CATEGORY PERSONAL DATA or SENSITIVE PERSONAL DATA

Where the Association processes Special Category Personal Data or Sensitive Personal Data, it must do so in accordance with one of the following grounds for processing;

- The Data Subject has given has given explicit consent to the processing of this data for a specified reason
- Processing is necessary for carrying out obligation or exercising rights related to employment or social security
- Processing is necessary to protect the vital interest of the Data Subject or, if the Data Subject is incapable of giving consent, the vital interests of another person
- Processing is necessary for the establishment, exercise or defence of legal claims or whatever court are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest

10.0 DATA SHARING

In order to ensure that it's to day activities are carried out in line with its policies and procedures, the Association shares its data with various third parties. In order to monitor that these third parties comply with data protection law, the third party organisations will be required to enter into an agreement with the Association. This agreement will govern the processing of data, security measures to be implemented and responsibilities of breaches.

Personal Data may be shared amongst the Association and third parties who require to process Personal data that the Association also processes. Both the Association and the third will be regarded as processing that data in their individual capacities as Data Controllers.

Where the Association shares in the processing of Personal Data with a third party it shall require the third party organisation to enter in a Data Sharing Agreement with the Association.

11.0 DATA PROCESSING

Some of the Association's activities such as payroll, maintenance & repair works) may be outsourced to a third party that processes Personal data on the Association's behalf. These third party entities are Data Processors.

Data Processors must comply with Data Protection laws and must ensure that they;

- Have appropriate technical security measures in place
- Maintain records of processing activities
- Notify the Association if there is a data breach

Where a Data Processor wishes to sub-contract their processing, they must obtain prior written consent from Association. The Data Processor will be liable in full for any Data protection breaches of the sub-contractor.

Where the Association contract with a third party to process personal data held by the Association, the third parties will be required to enter into a Data Protection Addendum with the Association (Appendix 3).

12.0 DATA STORAGE & SECURITY

All Personal Data held by the Association either electronically or in paper format must be held securely.

12.1 Paper Storage

It is the responsibility of employees to ensure that Personal Data stored on paper is;

- Kept in a secure place where unauthorised personnel cannot access it
- Not left where unauthorised personnel can access it
- Properly disposed of when it is no longer required

Personal data that is required to be retained on a physical file should be securely affixed to the file and the file stored securely.

12.2 Electronic Storage

Personal data stored electronically must also be protected from unauthorised use and access.

Personal data should be password protected when being sent internally or externally to the Association's data processors or third parties that have a Data Sharing Agreement with the Association.

Where Personal Data is stored on removable media such as CDs, DVDs or USB memory sticks, the removable media must be securely stored when not being used.

Personal Data should not be saved directly onto mobile devices and should only be stored on designated drivers and servers.

13.0 REPORTING DATA BREACHES

A Data Breach can occur at point when handling and processing Personal Data. The Association has legal duties regarding the reporting of a Data Breach or a potential breach occurring. Where the breach poses a risk to the rights and freedoms of the individual who is subject of the breach, the Association is required to report the breach externally in accordance with this policy.

13.1 Internal Reporting

Charing Cross Housing Association takes the security of the data it holds very seriously and will take all reasonable steps to keep data safe and secure.

In the unlikely event that a breach occurs the employee will report the breach or potential breach to the Data Officer as soon as it has occurred if possible but no later than 6 hours afterwards.

The report must be made in writing detailing the nature of the breach, how it occurred and the likely impact of the breach on the Data Subject(s)

On notification of a breach or potential breach the Association will;

- Take all reasonable steps available to contain the breach
- Consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and the Data Subjects affected
- Where appropriate, report the breach in accordance with this policy

- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

13.2 External Reporting to the ICO

13.2.1 Reporting to the ICO

The Association is required to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the ICO within 72 hours of the breach occurring.

13.2.2 Reporting to the Data Subjects

Where appropriate Data Subjects affected by the breach will be notified as soon as reasonably possible.

14.0 THE DATA OFFICER

The Association's Data Officer will be responsible for:

- Monitoring the Association's compliance with the law as well as its Data Protection policies
- Co-operating with the ICO and will serve as the Association's contact on matters concerning GDPR and date protection
- Reporting breached or suspected breached to the ICO and Data Subjects in accordance with this policy

15.0 THE RIGHTS OF DATA SUBJECTS

Data Subjects have a number of rights provided to them under the GDPR including the right to;

- View the Personal Data held about them by the Association whether in written or electronic form
- Request a restriction of processing their data
- Be forgotten
- Object to the Association's processing of their data

These rights are notified to the Association's tenants and other customers in the Fair Processing Notice.

15.1 Subject Access Requests

Data Subjects are entitled to view the data the Association hold on the by making a Subject Access Request.

When a Subject Access Request is received the Association must:

- Respond within one month of the date of receipt of the request
- Provide the Data Subject with an electronic or hard copy of the Personal Data requested unless any exemption to the provision of that data applies in law
- Identify where the Personal Data requested comprises of data relating to another Data Subject and take reasonable steps to obtain consent to disclose that Personal Data from those Data Subjects

Where the Association does not hold the Personal data requested, this must confirmed in writing as soon as practically possible but no later than one month from the date the request was made.

15.2 The Right To Be Forgotten

A Data Subject can exercise their right to be forgotten by submitting a request in writing to the Association that it erases the Data Subject's Personal Data in its entirety.

The Association will consider each request received on its own merit and, where appropriate will obtain legal advice. It shall be the responsibility of the Data Controller to accept or refuse the request and convey the decision in writing to the Data Subject.

15.3 The Right To Restrict or Object to Processing

A Data Subject may request in writing that the Association restrict its processing of the Data Subject's Personal Data or object to the processing of that data.

The Data Subject has an absolute right to objects to the processing of their personal data for any direct marketing activities undertaken by the Association and, if a written request to cease processing for this purpose is received, the Association must comply with the request immediately.

The Association will consider each request received on its own merit and, where appropriate will obtain legal advice. It shall be the responsibility of the Data Controller to accept or refuse the request and convey the decision in writing to the Data Subject.

16.0 PRIVACY IMPACT ASSESSMENTS (PIAs)

Before undertaking a projects or processing activity which poses a 'high risk' to an individual's privacy, the Association will carry out a Privacy Impact Assessment. 'High Risk' can include, but is not limited to, activities that use information relating to health or the implementation of a new IT system for storing and accessing Personal Data.

When carrying out a PIA, the Association will include:

- A description of the processing activity
- The purpose of the processing activity
- An assessment of the need for the processing
- A summary of risk identified
- The measures that will be taken to reduce those risk
- Details of any security measures required to be taken to protect the Personal Data

Where a PIA identifies a high level of risk which cannot be reduced, the Data Controller will notify and consult with the ICO within 5 working days.

17.0 ARCHIVING, RETENTION & DESTRUCTION OF DATA

The Association recognises that it is neither desirable nor practical to store and retain Personal Data indefinitely. It also must ensure that Personal Data is only retained for the period necessary. It shall therefore ensure that Personal Data is destroyed when it is no longer required and/or within the periods specified schedule contained in the Association's Document Retention & Disposal Policy.

18.0 POLICY REVIEW

This policy will be reviewed in full every 3 years. However amendments can be made at any time during that period as required and approved by the Management Committee.