Data Protection Policy

Reference	CS-CC-02
Information Classification	Public
Review Frequency	3 years
Date Reviewed/Approved	December 2019
Next Review Due Date	December 2022
Applicable Committee(s)	Management Committee
Owner - role	Corporate Compliance Officer

Record of Updates/Changes			
Current Version	**Date Approved**	**Approved By**	**Changes**

1. INTRODUCTION

Castlehill Housing Association (CHA) is committed to ensuring the secure and safe management of data held by CHA.

CHA needs to gather and use certain information about individuals. These individuals can include customers (tenants, factored owners etc.), employees and other individuals that CHA has a relationship with. CHA manages a significant amount of data including personal data and sensitive personal data (known as special category personal data under the GDPR and the Data Protection Act 2018).

This Policy sets out CHA's duties in processing data collected and managed by Castlehill Housing Association including by Castlehill Solutions and Castlehill Housing Trust.

2. LEGISLATIVE AND REGULATORY FRAMEWORK

It is a legal requirement that CHA process data correctly. CHA must collect, handle and store personal information in accordance with relevant legislation.

The relevant legislation in relation to the processing of data is:

- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Privacy and Electronic (EC Directive) Regulations 2003 (as may be amended by the proposed Regulations on Privacy and Electronic Communications)

Principles of Data Protection

As Data Controller, CHA shall be able to demonstrate compliance with the Data Protection Principles, as set out in the GDPR, that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner not compatible with those purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and kept up to date, where necessary taking every reasonable step to have it rectified or erased where it is found to be inaccurate
5. Kept no longer than is necessary in a form that allows identification of a Data Subject – personal data may be stored for longer for statistical or research purposes provided there are adequate security measures in place
6. Processed in a manner that ensures appropriate security, including safeguarding against breach

Definitions of Personal Data

For the purposes of this Policy, the following definitions will apply:

Personal data means data that relates to a living individual (data subject) who can be identified:

- From that data, or
- From that data and other information which is in the possession of, or is likely to come into the possession of CHA and
- Includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual

Special Category data is data that is held that can be used to identify an individual's

- Racial or ethnic origin
- Political opinions and trade union membership
- Religious or philosophical beliefs
- Biometric or genetic data
- Physical or mental health or condition
- Sexual life or sexual orientation

The Association has procedures for ensuring that all personal data is held and processed in accordance with the GDPR.

Processing of Personal Data

CHA is permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (please see further information below)
- Processing is necessary for the performance of a contract between CHA and the data subject or for entering into a contract with the data subject
- Processing is necessary for CHA's compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of CHA's official authority or
- Processing is necessary for the purposes of legitimate interests

Consent

Consent, as a ground of processing should be used by CHA where no other alternative ground for processing is available. In the event that CHA requires to obtain consent to process a data subject's personal data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a consent form if willing to consent. Any consent to be obtained by CHA must be for a specific and defined purpose i.e. general consent cannot be sought.

Processing of Special Category Personal Data

In the event that CHA processes special category personal data, CHA must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose
- Necessary for carrying out obligations or exercising rights related to employment or social security
- Necessary to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent
- Necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity
- Necessary for reasons of substantial public interest
- Processing relates to personal data which are manifestly made public by the data subject

Image Consent

CHA publishes images on the website, in leaflets and in other publications such as the Annual Performance Report. Any photograph of a tenant, customer, contractor, or staff member requires consent from the Data Subject. This is recorded separately, and stored centrally until such time as permission to use the image is withdrawn by the Data Subject or, in the case of staff consent for internal photographs, when the employment contract comes to an end.

As with all consent under the GDPR, consent to use the image can be withdrawn. This means that no publication published after consent is withdrawn will contain that image, and CHA's website will be updated where it is practical to do so.

Fair Processing Notice

CHA's Fair Processing Notice, available on our website, sets out the personal data processed by CHA and the basis for that processing. It informs data subjects of their rights, and who to contact to complain about Data Protection.

The Fair Processing Notice is provided to all of CHA's customers at the outset of processing their data.

A separate Fair Processing Notice is provided to all CHA employees, those applying for a vacant post, members and Management Committee members.

3. DATA STORAGE

All data held by CHA must be stored securely, whether in paper or electronically. CHA has an Information Security policy in place to ensure there are robust measures in place to protect personal data that is in electronic format.

All departments have a personal data register in place. This describes where personal information in the department is stored, how it is kept secure, and when the information is disposed of in order to adhere to the document retention schedule.

It is the responsibility of all staff to ensure that personal data is kept secure during their day-to-day duties and to ensure compliance with the Clear Desk Policy. Staff are trained to have awareness of good practice in personal data handling to reduce the risk of personal data breaches. All hard copy personal information is disposed of via confidential waste bins provided at each office location.

Security

CHA employees are authorised to access and use data only so far as it is appropriate for their jobs. Any data, whether manual or electronic, will have access restricted on that basis. System access for all team members is authorised by Line Managers.

Paper Storage

If personal data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no personal data is left where unauthorised personnel can access it. When the personal data is no longer required, it must be disposed of by the employee so as to ensure its destruction. If the personal data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with CHA's storage provisions.

Electronic Storage

Personal data stored electronically must also be protected from unauthorised use and access. CHA's IT Provider have a system for ensuring that all portable storage devices, including mobile phones and laptops, have an appropriate level of security in place to avoid inadvertent breaches or inappropriate access, including password protection when not in use.

Personal data should be password protected when being sent internally or externally to CHA's data processors or those with whom CHA has entered into a Data Sharing Agreement. If personal data is stored on removeable media (CD, DVD, USB memory stick) then that removeable media must be stored securely at all times when not being used. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

Data Retention Schedule

The data retention schedule determines the time period beyond which personal data will no longer be retained. The Data Protection Officer and the appropriate Departmental Managers are responsible for ensuring that data held beyond the time limits set out in the retention schedule is confidentially and satisfactorily destroyed.

4. ROLES AND RESPONSIBILITIES

The ultimate responsibility for the implementation and compliance of the Data Protection Policy lies with the Management Committee and is delegated to the Chief Executive.

All Directors are responsible for ensuring that departments and working practices comply with this Policy and for raising issues of non-compliance with the Data Protection Officer. Any relevant actions on Data Protection will be included in Departmental Workplans which are reviewed by the relevant subcommittee.

Department Managers have responsibility for identifying, recording and reviewing any personal data held by their department, both in paper and electronic form. It is their responsibility to verify information to ensure it is accurate and not held beyond a reasonable length of time. A full register of the personal data held in each department, and indicative timescales for data and document retention, is held centrally. This is a live document and is updated and approved by Departmental Managers on at least an annual basis.

Managers are also responsible for ensuring their teams are aware of their duties in relation to Data Protection.

The Corporate Compliance Officer is identified as the Data Protection Officer and is responsible for ensuring compliance by CHA with Data Protection legislation. The Data Protection Officer's contact details are noted on CHA's website and contained within the Fair Processing Notice. The Data Protection Officer is responsible for:

- Monitoring CHA's compliance with Data Protection legislation and this Policy
- Co-operating with, and serving as CHA's contact for discussions with the Information Commissioner's Office (ICO)
- Reporting breaches or suspected breaches to the ICO and data subjects

All staff in CHA deal with some level of personal information and all staff have a responsibility to understand their obligations for dealing with data and to be aware of this Data Protection Policy.

5. TRAINING

Staff are required to have an understanding and appreciation of the principles of GDPR. The staff handbook contains a statement on the Policy – however, all staff are required to read the full policy.

Mandatory training should be completed by all relevant staff to reinforce the importance of both DP and confidentiality. For existing staff, this will be completed on a regular basis to be reviewed by the Senior Management Team (SMT) and all new staff will complete this training as part of their induction.

6. DATA SHARING

CHA shares data (in accordance with Data Protection legislation) with various third parties for numerous reasons in order that its day to day activities are carried out in line with CHA's relevant policies and procedures. In order that CHA can monitor compliance by these third parties with Data Protection laws, CHA will require the third party organisations to enter in to an Agreement with CHA governing the processing of data, security measures to be implemented and responsibility for breaches.

If there are any doubts about whether sharing data is appropriate, this is discussed with CHA's Data Protection Officer. If it is likely that sharing will occur on a regular basis, then consideration should be given to creating a more formal Information Sharing Protocol.

Data Subject Rights

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by CHA, whether in written or electronic form.

Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to CHA's processing of their data. These rights are notified to CHA's tenants and other customers in CHA's Fair Processing Notice.

Subject Access Requests

Data Subjects are permitted to view their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, CHA must respond to the Subject Access Request within one month of the date of receipt of the request. CHA:

- Must 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
- Where the personal data comprises data relating to other data subjects, CHA must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request or
- Where CHA does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to CHA seeking that CHA erase the data subject's personal data in its entirety.

Each request received by CHA will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The Data Protection Officer will have responsibility for accepting or refusing the data subject's request in accordance with this policy and will respond in writing within 30 days of the request being received.

The Right to Restrict or Object to Processing

A data subject may request that CHA restrict its processing of the data subject's personal data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by CHA, a data subject has an absolute right to object to processing of this nature by CHA, and if CHA receives a written request to cease processing for this purpose, then it must do so immediately.

Each request received by CHA will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The Data Protection Officer will have responsibility for accepting or refusing the data subject's request in accordance with the policy and will respond in writing within 30 days of the request being received.

7. PRIVACY IMPACT ASSESSMENTS (PIAS)

These are a means of assisting CHA in identifying and reducing the risks that our operations have on personal privacy of data subjects.

CHA shall:

- Carry out a PIA before undertaking a project or processing activity which poses a 'high risk' to an individual's privacy. High risk can include, but is not limited to, activities using information

relating to health or race, or the implementation of a new IT system for storing and accessing personal data and

- In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks and details of any security measures that require to be taken to protect the personal data

CHA will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Data Protection Officer within five working days.

8. BREACHES

A data breach can occur at any point when handling personal data and CHA has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally.

Internal Reporting

CHA takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the DPO must be notified in writing of (i) the breach, (ii) how it occurred and (iii) what the likely impact of that breach is on any data subject(s)
- CHA must seek to contain the breach by whatever means available
- The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with 'Reporting to the ICO' section below
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

Reporting to the ICO

The DPO will require 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 Information Commissioner's Office (ICO) within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

The DPO will be responsible for:

- Monitoring the Association's compliance with Data Protection laws and this Policy
- Co-operating with and serving as the Association's contact for discussions with the ICO
- Reporting breaches or suspected breaches to the ICO and data subjects in accordance with the procedure.

9. MONITORING & REVIEW

Individual departments are responsible for maintaining records of the data they hold. They will update the Data Protection Officer as to any changes to their processes. They will review their personal data management on at least an annual basis to ensure compliance with the GDPR.

The Policy will be reviewed at least every 3 years, or following significant changes in legislation.