Data Protection Policy

Reference	CS-CC-02
Information Classification	Public
Review Frequency	3 years
Date Reviewed/Approved	September 2026
Next Review Due Date	September 2029
Applicable Committee(s)	Management Committee
Owner - role	Compliance Advisor

Record of Updates/Changes			
Current Version	**Date Approved**	**Approved By**	**Changes**
1.	25/10/21	Management Committee	
2.	28/10/24	Management Committee	Updated references. Removed Appendices 1-4 (Fair Processing Notices & Template Data Sharing Agreements). Teams Transcription section added. Image consent section added. Updated section on electronic storage of personal data. Updated section on data sharing.
3.	Sept 2026		Policy updated in accordance with SFHA model documents to reflect changes introduced by the Data (Use and Access) Act 2025

1. INTRODUCTION

Castlehill Housing Association (CHA) is committed to ensuring the secure and safe management of data held by CHA in relation to customers, staff and other individuals. CHA's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

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, from a variety of sources. This data contains personal data and sensitive personal data (known as special categories of personal data under the UK General Data Protection Regulation).

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. The purpose of this Policy is to set out the procedures for the management of such data.

2. LEGISLATION

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

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

- UK General Data Protection Regulation ('the GDPR')
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Data Protection Act 2018 ('the 2018 Act') and
- Any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 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. DATA

CHA holds a variety of Data relating to living individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects and relates to them is known as Personal Data. The Personal Data held and processed by CHA is detailed within Fair Processing Notices.

"Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by CHA and which relates to that individual

CHA also holds Personal Data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data". The Secretary of State may designate further categories of Special Category Personal Data and if this occurs CHA shall treat any such designated data accordingly.

4. PROCESSING OF PERSONAL DATA

"Processing" is defined very broadly and encompasses any operation performed on or with personal data, including but not limited to collection, recording, organisation, structuring, storage, adaptation/alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In effect, it is any activity involving personal data.

CHA must ensure that all processing activities comply with the UK GDPR principles of lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality and accountability.

Employees with access to and responsibility for personal data must access only data that they have authority to access and only for authorised purposes.

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 (see consent clause 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 official authority;
- Processing is necessary for the purposes of legitimate interests pursued by CHA or by a third party – note that this condition is not available to public bodies as defined in the relevant legislation or
- Processing is necessary for the purposes of a recognised legitimate interest

The above conditions are in line with Article 6 of the UK General Data Protection Regulation.

Fair Processing Notice

CHA has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by CHA. That FPN is provided to the customers from the outset of processing their Personal Data and they are advised of the terms of the FPN when it is provided to them. If CHA receives personal data about an individual from another source (so not from the individual direct) CHA will provide the required privacy information in accordance with the requirements of Data Protection Law.

The Fair Processing Notice sets out the Personal Data processed by CHA and the legal basis for that Processing. It informs Data Subjects of their Rights and who to contact to complain about Data Protection.

A copy of CHA's Fair Processing Notice can be found on CHA's website.

Employees

Employee Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by CHA. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to prospective Employees at application stage.

A copy of any employee's Personal Data held by CHA is available upon request by that employee from CHA's Data Protection Officer (see part 8) subject to certain exemptions.

Consent

Consent as a ground of processing will require to be used from time to time by CHA when processing Personal Data. It 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, (unless extenuating circumstances apply and except for Microsoft Teams Transcription – see below) 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 relevant consent form if willing to consent (again, subject to extenuating circumstances such as the Data Subject being unable to write). Any consent to be obtained by CHA must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

Transcription – Microsoft Teams

An exception to the requirement for a written, signed consent form is where a written transcript is taken of a call/meeting through Microsoft Teams.

Transcription is an automatically generated, recorded (written) text of what was said in a call. Callers/meeting attendees will require to provide their explicit consent prior to a transcript being taken.

Image Consent

CHA publishes images on the website and in leaflets/publications. Any photograph of an individual requires written consent from the Data Subject. Consent to use the image can be withdrawn at any time.

Processing of Special Category Personal Data or Criminal Offence Data

In the event that CHA processes Special Category Personal Data or Criminal Offence Data, CHA must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following

1. The data subject has given explicit consent to the processing of this data for a specified purpose;
2. Processing is necessary for carrying out obligations or exercising rights related to employment, social security, or social protection law;

3. 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;
4. Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity;
5. Processing is necessary for reasons of substantial public interest under law and
6. Processing is necessary for health or social care.

All the grounds for processing sensitive personal data are set out in the GDPR and expanded on in the Data Protection Act 2018.

5. DATA STORAGE AND SECURITY

All Personal Data held by CHA must be stored securely, whether electronically or in hard copy format.

Paper Storage

If Personal Data is stored on paper, it will be kept in a secure place where unauthorised personnel cannot access it. In accordance with internal policy, employees will ensure that no Personal Data is left in a place where unauthorised personnel can access it. When the Personal Data is no longer required (and CHA has a Retention Schedule which sets out the expected timescales for holding various categories of personal data) it must be disposed of by the employee so as to ensure its secure 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.

All electronic storage, transfer and disposal of data is carried out in accordance with CHA's internal Information Security Policy and Procedures.

5.1 DATA SHARING

CHA shares its data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with CHA's relevant policies and procedures.

In order that CHA can monitor compliance by these third parties with Data Protection laws, CHA may require the third party organisations to enter into an Agreement with CHA governing the processing of data, security measures to be implemented, and responsibility for breaches.

There is a Model Data Sharing Agreement which CHA may use in such scenarios. However CHA will determine on a case-by-case basis what the most appropriate contract terms (if required) shall be.

Processors

A processor is a third-party entity that process Personal Data on behalf of CHA and is frequently engaged if certain of CHA's work is outsourced (e.g. payroll, maintenance and repair works).

A processor must comply with Data Protection laws. CHA's processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify CHA if a data breach is suffered.

If a processor wishes to sub-contract their processing, CHA's prior written consent must be obtained. Upon a sub-contracting of processing, the processor will be liable in full for the data protection breaches of their sub-contractors.

Where CHA contracts with a third party to process personal data held by CHA, it shall require the third party to enter in to a written contract with CHA with such contract outlining, amongst other things, how personal data will be kept safe and secure. CHA has a model Data Protection Addendum and model Data Processing Clauses which can be used in these scenarios. But CHA may, on a case-by-case basis, determine that other contract wording is appropriate.

6. 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 it becomes known the breach or potential breach has occurred, , CHA's 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 whichever means available;
- The DPO must consider whether the breach is one which requires to be reported to the IC and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements, Data Processing Agreements or equivalent contract terms

Reporting to the IC and to Data Subjects

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 Commission (IC) within 72 hours of the breach occurring or CHA becoming aware of the breach. The DPO must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

Where a breach poses a *high* risk to the rights and freedoms of the Data Subjects impacted by the breach, CHA must, in addition to notifying the IC, promptly notify the Data Subjects in question.

7. DATA PROTECTION OFFICER ('DPO')

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. CHA has appointed a Data Protection Officer

(DPO). CHA's DPO's details are noted on CHA's website and contained within the Fair Processing Notice.

The DPO will be responsible for:

- Monitoring CHA's compliance with Data Protection laws and this Policy and advising on compliance as needed;
- Co-operating with and serving as CHA's contact for discussions with the IC
- Reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

8. DATA SUBJECT RIGHTS

Certain rights are provided to Data Subjects under Data Protection Law:

- A right to be informed about the collection and use of their personal data (typically fulfilled by providing individuals with a Fair Processing Notice) (the "right to be informed"):
- A right to access and receive a copy of their personal data, plus other supplementary information (the "right of access")
- A right to have inaccurate personal data rectified and incomplete personal data completed (the "right to rectification")
- A right to have personal data erased (the "right to erasure")
- The right to request the restriction or suppression of personal data (the "right to restrict")
- The right to obtain and reuse certain personal data across different providers (the "right to data portability")
- The right, in certain circumstances, to object to processing of their data (the "right to object")
- The right to make a complaint about how their personal data has been processed (the "right to complain") and
- Rights to protect individuals against automated decision making or profiling ("rights related to automated decision making")

These rights are notified to CHA's tenants and other customers in CHA's Fair Processing Notice. Such rights are subject to qualification and are not absolute.

The Right of Access: Subject Access Requests

Data Subjects are permitted to view their Personal Data held by CHA upon making a request to do so (a Subject Access Request) subject to certain exemptions. Upon receipt of a request by a Data Subject, CHA must respond to the Subject Access Request within one month from the day after the date of receipt of the request (unless CHA is entitled under the relevant legislation to increase this timescale). 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 shall only release that data where: CHA has obtained consent from those Data Subjects or CHA determines it is reasonable to disclose said data without consent. Or
- where the Association does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

The Right to Erasure

A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request 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 DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

Requests for Erasure will be considered and responded to by CHA by one month from the day after the date we receive the request unless CHA is entitled to increase the timescales under relevant legislation.

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 DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

The Right to Rectification

A Data Subject may request CHA to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request CHA to have incomplete Personal Data completed.

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 DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

The Right to Data Portability

A Data Subject may ask for their personal data which they have provided to CHA to be provided in a structured, commonly used, machine readable format or the Data Subject may ask for this data to be transmitted directly to another organisation. This is subject to certain exemptions.

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 DPO will have responsibility for accepting or refusing the Data Subject's request in accordance with clause 9 and will respond in writing to the request.

The Right to Complain

A Data Subject may complain to CHA if they consider their personal data has been processed by CHA in contravention of Data Protection Law.

Any such complaint shall be handled in accordance with CHA's Data Protection Complaints Process.

Rights related to Automated Decision Making

Should CHA utilise any automated decision making it shall follow the requirements set down in data protection law to protect the Data Subjects in question.

9. PRIVACY IMPACT ASSESSMENTS ('PIA's)

These are a means of assisting CHA in identifying and reducing the risks that our operations have on personal privacy of Data Subjects. Whilst this Policy uses the term PIAs, it is also recognised that these assessments are also commonly referred to as "Data Protection Impact Assessments" or similar.

CHA shall:

i. Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual. 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
ii. 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 IC in the event that a PIA identifies a high level of risk which cannot be reduced or mitigated. The DPO 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 DPO within five (5) working days.

10. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

CHA cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary.

CHA shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within CHA's data retention schedule at Appendix 1 hereto.

APPENDIX ONE – TABLE OF DURATION OF RETENTION OF CERTAIN DATA

The table below sets out retention periods for Personal Data held and processed by the Association. It is intended to be used as a guide only. The Association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Type of record	Department	Suggested retention time
Governance documentation	Corporate Services	Permanently
Committee membership records	Corporate Services	5 years from last contact after membership ceases
Committee meeting minutes/papers	Corporate Services	Permanently
Committee member annual reviews	Corporate Services	Current year plus 2 years
Annual returns to the regulator	Housing Management & Corporate Services	5 years
Strategic Plans	Chief Executive	5 years after plan completion
Accounting records	Finance	6 years
Bank statements and reconciliations	Finance	6 years
Audit Reports (Internal and External)	Finance / Corporate Services	6 years from completion of audit
Responses to requests for information / personal data	Corporate Service	Last action plus 6 years
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	Finance	6 years from the date of the redundancy
Payroll information – staff payments and deductions, reports and payments to HMRC, , tax code notices, taxable	Finance - Payroll	3 years after the end of the tax year they relate to

expenses or benefits and payroll giving scheme documents including agency contract and employee authorisation forms		(Staff pay details including expenses to be kept in payroll file for 5 years from termination of employment)
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	Finance - Payroll	3 years after the end of the tax year to which they relate
Income tax, NI returns, correspondence with tax office	Finance	At least 3 years after the end of the tax year to which they relate
Pension scheme information – scheme return, notifiable events, late payment of contributions, breaches of law	Finance	6 years from end of the scheme year in which the event took place
Accident books and records and reports of accidents	H&SMG/Department Heads	3 years after the date of the last entry
Health and Safety assessments and records of consultations with safety representatives and committee	H&SMG/Department Heads	Permanently
Documents relating to successful tenders	Department Heads/Managers	6 years from end of contract
Signed contract		6 years from end of contract
Documents relating to unsuccessful form of tender	Department Heads/Managers	1 year after notification
Applications for accommodation	Thesehomes /Housing Management	5 years after offer accepted

Tenancy files	Housing Management & Castlehill Housing Trust	Duration of tenancy and key information from former tenancy files for 5 years
Lease documents	Housing Management	5 /12/15 years after lease termination
Residents' meeting minutes	Housing Management	1 year
Minute of factoring meetings	Housing Management /Property Services	Duration of appointment
Sheltered Housing support plans	Housing Management	Duration of tenancy and key information from former tenancy files for 5 years
Sheltered Housing daily contact sheets	Housing Management	Duration of tenancy and key information from former tenancy files for 5 years
Key Project contact information sheet	Key Project	Duration of tenancy and key information from former tenancy files for 5 years
Service user case files	Care & Repair	2 years from closure of case
Occupational Therapy referrals	Property Services	2 years
Records relating to working time – including annual leave/holiday pay and sick leave	Corporate Services	6 years from the date they were made
Personnel files – including pay details	HR	5 years from termination of employment except: • Emergency contact details, reference contacts, references and lone worker scheme documents – destroyed following end of employment • Maternity/Paternity/Adoption/Sick Leave – destroyed 3 years following end of employment) • Records relating to working time – destroyed 6 years from the date they were made • Documents proving the right to work in the UK – 2 years after employment ceases
Recruitment application forms, interview notes	HR	A year from date of interviews. Successful applicants' documents should be transferred to personnel file

Timesheet and leave details	HR	6 years from termination of employment