

Data Protection Policy

Document Ref:	CHG08
Revision No.	2.1
Date approved:	10 September 2024
Related documents:	Compliance Statement, Privacy Statement, SAR Procedure, Data Breach Procedure, Data Sharing Protocol

1 Purpose

- 1.1 The Data Protection Policy sets out Cromwood Housing Limited (CHL) commitment to protecting personal data, and how it implements that commitment concerning the collection and use of personal data in line with the legal requirements.

2 Introduction and aims

- 2.1 CHL's policy is to ensure that everyone who has dealings with CHL has a right to privacy and to expect that all personal information about them will be handled sensitively and with due regard to its confidentiality.
- 2.2 This policy covers, but is not limited to, personal data and special categories of personal data as defined by GDPR.
- 2.3 Personal data is defined as any information relating to an identified or identifiable living person ('data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that living person.
- 2.4 Special categories of personal data is separately defined within the GDPR and covers racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation.
- 2.5 CHL will:
- 2.5.1 comply with the law regarding the protection and disclosure of information, treat all personal and sensitive organisational information as confidential.
 - 2.5.2 not disclose personal information without the prior express consent of the individual concerned, except in the circumstances outlined below in the section on disclosure.
 - 2.5.3 not gain or attempt to gain access to unauthorised information.
- 2.6 All staff have a duty to respect confidentiality of personal information held by CHL. In meeting this duty staff are expected to exercise judgment and common sense.

2.7 CHL has nominated a member of staff to act as CHL Data Protection Officer (DPO). The DPO for the CHL Group is the Strategic Director. All enquiries regarding data protection must be passed to the DPO.

2.8 The GDPR is enforced by the Information Commissioners Office which has extensive powers under the GDPR to take action against organisations which breach data protection law. This includes substantial fines as well as other regulatory action such as enforcement notices.

3 Policy Statement

3.1 Employees and residents have a right to view personal information about themselves and their family. They are entitled to know:

3.1.1 what data is held or otherwise processed about them;

3.1.2 the purposes of the processing;

3.1.3 the categories of personal data concerned;

3.1.4 the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

3.1.5 where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

3.1.6 the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

3.1.7 the right to lodge a complaint with the ICO;

3.1.8 where the personal data is not collected from the data subject, any available information as to their source;

3.1.9 the existence of automated decision-making, including profiling and in those cases at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3.2 CHL will only process personal data if one or more of the conditions set out in Article 6 of the GDPR have been satisfied. The relevant conditions for CHL's activities are:

3.2.1 processing is necessary for the purposes of the legitimate interests pursued by CHL or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the resident or employee which require protection of personal data, in particular where the data subject is a child.

3.2.2 the express consent of the resident or employee is obtained prior to the processing of personal data. Consent must be freely given; it must also be specific and informed. It must be given by an unambiguous statement or by clear affirmative action signifying the data subject's agreement to the processing. In practice this means that wherever possible consent should be

obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, verbal consent can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept.

- 3.2.3 processing is necessary for the performance of a contract to which the resident or employee is party or in order to take steps at the request of the resident or employee prior to entering the contract;
 - 3.2.4 processing is necessary for compliance with a legal obligation to which CHL is subject; and
 - 3.2.5 processing is necessary in order to protect the vital interests of the resident or employee or of another natural person.
- 3.3 Personal information – especially special categories personal information – about employees and residents is shared only with staff who need to know the information in order to carry out their legitimate duties. This may involve sharing information between individuals in different departments. Where appropriate, CHL sets up protocols to clarify how this operates in practice to ensure that only those people who have a need to know are able to access personal data of employees or residents.
- 3.4 CHL will only collect and process special categories personal data if one of the conditions set out in Article 9 of the GDPR or Schedule 1 of the Data Protection Act 2018 have been satisfied. The relevant conditions for CHL's activities are:
- 3.4.1 the data subject has given explicit consent to the processing of the personal data for one or more specified purposes. Consent must be freely given as set out in clause 3.2 (Article 9 GDPR);
 - 3.4.2 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law and the controller has an appropriate policy document in place (Article 9 and Schedule 1 DPA 2018);
 - 3.4.3 processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent (Article 9);
 - 3.4.4 processing relates to personal data which have been made public by the data subject (Article 9);
 - 3.4.5 processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (Article 9);
 - 3.4.6 processing is necessary for reasons of substantial public interest. (The only categories in this subsection potentially relevant to CHL are the administration of justice (i.e. providing information to the Court or those pursuing proceedings) ; and preventing or detecting unlawful acts) (Article 9 and Sch 1 DPA 2018);
 - 3.4.7 processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of

health or social care or treatment or the management of health or social care systems and services (Article 9 and Schedule 1 DPA 2018).

- 3.5 These conditions are little changed from those which applied under Schedule 3 Data Protection Act 1998 and the Data Protection (Processing of Sensitive Personal Data) Order 2000.

4 Right of Access to Personal Information

- 4.1 In addition to their rights under this policy all of CHL's employees and residents and anyone else in respect of whom personal data is processed have a right to ask CHL, under the GDPR, for personal information held about them and this section details the information they are entitled to see under the GDPR.
- 4.2 The rights of our employees and residents under the GDPR are set out here for completeness (see also CHL's Subject Access Request Procedure which explains why it is more appropriate to make a subject access request), within one month of a written request a data subject is entitled to:
- 4.2.1 be told whether personal data, of which he or she is the subject, is held in CHL's records, or otherwise processed by CHL;
 - 4.2.2 be given a description of the personal data, the purpose for which the data is being or may be processed and the persons or classes of persons to whom the data has been or may be disclosed;
 - 4.2.3 have communicated to them in an intelligible form the information constituting the personal data held about them and any available detail as to the source of that information;
 - 4.2.4 be told the envisaged period for which the data will be stored or, if not possible, how it will be decided when it will be destroyed;
 - 4.2.5 be informed of their right to erasure of personal data; the right to object to processing; the right to rectification of data; to restriction on processing; and the right to object to processing;
 - 4.2.6 be informed of their right to complain to the ICO; and
 - 4.2.7 know of the existence of any automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

5 Access to Personal Information Refused

- 5.1 CHL reserves the right to refuse the employee or resident access to information if:
- 5.1.1 it would identify another individual who has not consented to the disclosure Note: organisations are not covered by GDPR so information about them may be disclosed. However, to avoid any claims of breach of confidentiality, their consent should be sought and disclosure should only be made without their consent if it cannot reasonably be obtained and it is reasonable in all the circumstances to make disclosure



- 5.1.2 it is legally privileged correspondence e.g. between CHL and its solicitors
- 5.1.3 the data is held for management forecasting or management planning if the disclosure is likely to prejudice that activity e.g. information about plans to promote, transfer or make a worker redundant
- 5.1.4 information containing details of CHL's intentions concerning negotiations with an employee may be withheld to the extent to which access would be likely to prejudice those negotiations
- 5.1.5 the information consists of a reference given or to be given in confidence by the employer for:
 - 5.1.5.1 the education, training or employment of the worker
 - 5.1.5.2 the appointment of the worker to any office
 - 5.1.5.3 the provision by the worker of any service
- 5.1.6 the information is held for:
 - 5.1.6.1 the prevention of the detection of crime; and/or
 - 5.1.6.2 the apprehension or prosecution of offenders; and/or
 - 5.1.6.3 the assessment or collection of any tax or duty or any other imposition of a similar nature where access would be likely to prejudice any of the above matters
 - 5.1.6.4 the information was provided in confidence by a third party e.g. social workers, doctors, solicitors, local councils or the DSS
 - 5.1.6.5 in the opinion of CHL or a health professional it would be likely to cause serious harm to the physical and/or mental health of a resident or another person;
 - 5.1.6.6 the information requested relates to non-personal details such as property records or maintenance details. The association is only obliged to provide access to personal information about the resident and sometimes about their family.

6 Disclosure

- 6.1 Disclosure of personal information outside CHL will only be made with the informed express consent of the individual concerned except:
 - 6.1.1 to comply with the law (e.g. the police, Inland Revenue, Council Tax Registration Officer, Social Security Fraud Act) or a court order
 - 6.1.2 where there is a clear health or safety risk to an individual or members of the public, evidence of fraud against CHL, other irregular behaviour or a matter CHL is investigating
 - 6.1.3 in connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g. applications for possession or for payment of Housing Benefit direct)

- 6.1.4 where CHL has entered into a formal protocol with the police or a local authority department; and
- 6.1.5 providing the name, address and contact number of a resident to contractors or other agents providing services on CHL's behalf.

7 Accuracy of Personal Information: right of rectification

- 7.1 An employee, resident, former resident or applicant for housing may challenge the information held by CHL on their particular file if they feel it to be incorrect and can provide evidence to support this.
- 7.2 The right of rectification under the GDPR (Article 16) entitles the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

8 Rights of erasure, restriction on/objection to processing and withdrawal of consent

Erasure

- 8.1 Under the GDPR the rights of data subjects are extended to give individuals more protection and greater control over their personal information.
- 8.2 The right to erasure is also known as 'the right to be forgotten'. This enables an employee or resident to request the deletion or removal of personal data where there is no compelling reason for its continued processing by CHL.
- 8.3 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals only have a right to erasure where:
 - 8.3.1 the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
 - 8.3.2 where the individual withdraws consent.
 - 8.3.3 where the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
 - 8.3.4 the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
 - 8.3.5 the personal data has to be erased in order to comply with a legal obligation.
 - 8.3.6 the personal data is processed in relation to the offer of information society services to a child.
- 8.4 CHL can refuse to deal with a request to erase where the personal data is processed for the following reasons:
 - 8.4.1 to exercise the right of freedom of expression and information;
 - 8.4.2 to enable functions designed to protect the public to be achieved e.g. government or regulatory functions

- 8.4.3 to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- 8.4.4 for public health purposes in the public interest;
- 8.4.5 archiving purposes in the public interest, scientific research historical research or statistical purposes;
- 8.4.6 the exercise or defence of legal claims; or
- 8.4.7 where the organisation has an overriding legitimate interest for continuing with the processing

Restriction on processing

- 8.5 A data subject has the right to require a controller to stop processing his/her personal data. When processing is restricted, CHL are allowed to store the personal data, but not further process it.
- 8.6 CHL will be required to restrict the processing of personal data in the following circumstances:
 - 8.6.1 Where an individual (usually but not solely, employees or residents) challenges the accuracy of the personal data, we must restrict processing until we have verified its accuracy
 - 8.6.2 Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.
 - 8.6.3 When processing is unlawful and the individual requests restriction instead of erasure.
 - 8.6.4 If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
 - 8.6.5 If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 8.7 We must inform individuals when we decide to remove the restriction giving the reasons why.

Objection to processing

- 8.8 Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public tasks/exercise of official authority; direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- 8.9 The only category relevant to CHL is where we process personal data for the purposes of our legitimate interests. In that case, where an individual (resident or employee) objects, we must stop processing the personal data unless:
 - 8.9.1 we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
 - 8.9.2 the processing is for the establishment, exercise or defence of legal claims.

Withdrawal of consent

- 8.10 An individual has the right to withdraw consent at any time.
- 8.11 If the basis on which personal information is being processed is the consent of the individual, then that processing must stop.
- 8.12 It may be that another reason for processing can be relied on such as legitimate interests.
- 8.13 In practice a withdrawal of consent is likely to be accompanied by a request to erase in which case CHL will need to rely on one of the other exceptions to erasure e.g. overriding legitimate interest.

9 Responsibilities

- 9.1 The Finance Director shall be responsible for managing and resourcing this policy, and monitoring its effectiveness

10 Performance, Monitoring and Evaluation

- 10.1 The Board shall receive a report in the event that data protection measures have failed. The Finance Director shall report periodically regarding the controls that are in place regarding the security of tenant data and how it might be improved.
- 10.2 This policy will be subject to review no later than three years from the date of approval, or sooner if a substantial change in circumstances requires.