CORNWALL HOUSING

# Data Protection Policy

A CORNWALL COUNCIL COMPANY

CORNWALL HOUSING

| Policy Title | CHL Data Protection Policy | | |
|---|---|---|---|
| Version | 3 | Status | Final |
| Date | 15/08/2023 | Author | Sue Allport |
| Next Review Date: | 15/08/2024 | | |
| Responsible Officer: | Jackie Noyes | | |
| Associated documents | XXXXXXXX | | |

## Key messages

The purpose of this document is to outline:

- How Cornwall Housing Ltd (CHL) will ensure compliance with the UK GDPR and Data Protection Act 2018.
- Explain the roles and responsibilities relevant to internal compliance
- How compliance with this policy will be monitored

### Does this policy relate to me?

This policy applies to all the processing of personal data carried out by (CHL) including processing carried out by joint controllers, contractors, and processors.

# 1. INTERPRETATION

### 1.1 Key Terms

**Data Controller**: the person or organisation that determines when, why and how to process personal data. We are the data controller of all personal data used in (CHL)

**Data Subject**: a living, identified or identifiable individual about whom we hold personal data.

**Data Privacy Impact Assessment (DPIA)**: an assessment to identify and reduce data protection risks of a data processing activity or project.

**Data Protection Act 2018**: The legislation which ratifies the GDPR in English law.

**General Data Protection Regulation (GDPR)**: the General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

**Personal Data**: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes the special categories of personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour. The GDPR and Data Protection Act 2018 apply to any information held about a living, identifiable individual.

**Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity, or availability of personal data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of personal data is a personal data breach.

**Privacy Notices**: notices setting out information that may be provided to data subjects when we collect information about them.

**Processing or Process**: any activity that involves the use of personal data. It includes obtaining, recording, or holding the data, or organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transmitting or transferring personal data to third parties.

**Special Categories of Personal Data**: personal data concerning racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

## 2. INTRODUCTION

2.1 This policy provides a framework for ensuring that Cornwall Housing Ltd (CHL) meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). Cornwall Housing is registered as a Data Controller with the Information Commissioner's Office (ICO) registration number Z7599901.

2.2 This policy applies to all personal data we process regardless of whether it is in electronic form or hard copy or whether it relates to past or present employees, customers, clients or supplier contacts, board members, volunteers, website users or any other data subject.

2.3 Our staff have access to a number of policies, operational procedures, and guidance to give them appropriate direction on the application of the data protection legislation.

- Retention and Disposal Policy
- Freedom of Information Guidance
- RARE requests (including SAR)
- Data Breach Guidance
- Equality and Diversity Policy

2.4 This policy is an internal document and should not be shared with third parties, clients, or regulators without prior authorisation from the Director of Resources.

2.5 This policy does not form part of any employee's contract of employment. We shall keep this policy under regular review and may amend it from time to time.

## 3. SCOPE

3.1 Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. We are exposed to potential fines of up to the higher of up to £17.5 million or 4% of total annual turnover for failure to comply with the provisions of the GDPR.

3.2 This policy applies to all employees, workers, contractors, volunteers, agency workers, consultants, Directors, and Officers and to any other third party who processes personal data on our behalf. You must ensure that you read, understand and comply with this policy when processing personal data as part of your work role.

3.3 The (CHL) Board has overall responsibility for the effective operation of this policy. The Director of Resources will oversee this policy. Please contact the Information Governance

Officer (IGO with any questions about the operation of this policy or if you have any concerns that this policy is not being or has not been followed.

## 4. REPORTING A BREACH

4.1 We have put in place procedures to deal with any suspected personal data breaches and will notify the data subject or the regulator (ICO) where we are legally required to do so. We maintain a record of all personal data breaches which will be reviewed regularly.

4.2 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the IGO and follow the CHL Data Breach Guidance (link to Guidance to be added here). You should preserve all evidence relating to the potential breach.

## 5. WHAT INFORMATION IS PROTECTED

5.1 Personal data includes any information relating to an identified or identifiable natural living person. There are two types of personal data under the UK GDPR, personal data, and special category data.

5.2 Personal data means any information relating to a living individual who can be identified from that information (a "data subject") or on its own when taken together with other information. This may include both facts and expressions of opinion about the person. It does not include anonymised data.

5.3 Special category data is more sensitive and afforded more protection under the UK GDPR. This includes information relating to:

- 5.3.1 Race or ethnic origin.
- 5.3.2 Political opinions.
- 5.3.3 Religious or philosophical beliefs.
- 5.3.4 Trade union membership.
- 5.3.5 Genetic data.
- 5.3.6 Health data.
- 5.3.7 Information relating to sexual life and/or sexual orientation; and
- 5.3.8 Criminal data (convictions and offences).

## 6. PERSONAL DATA PROTECTION PRINCIPLES

6.1 We ensure that we process all personal data in accordance with the data protection principles set out in the UK GDPR. Personal data must be:

- 6.1.1 processed lawfully, fairly and in a transparent manner.
- 6.1.2 collected only for specified, explicit and legitimate purposes.
- 6.1.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- 6.1.4 accurate and where necessary kept up to date. Any inaccurate data must be deleted or rectified without delay.
- 6.1.5 not kept for longer than is necessary for the purposes for which it is processed; and
- 6.1.6 kept secure and protected against unauthorised or unlawful processing and

against accidental loss, destruction, or damage

6.2 There is also an overarching principle of accountability. We must ensure that are responsible for complying with the UK GDPR and able to demonstrate this. We demonstrate our accountability by:

6.2.1 appointing a Director of Resources.
6.2.2 implementing privacy by design measures at the outset of processing personal data and completing data privacy impact assessments where high-risk processing is likely to be carried out.
6.2.3 putting in place suitable policies and privacy notices regarding our data processing activities.
6.2.4 providing annual training to our staff on data protection matters; and
6.2.5 by conducting periodic reviews and audits to assess our compliance with the UK GDPR.

## 7. LAWFULNESS OF PROCESSING

7.1 Personal data must be processed lawfully, fairly and in a transparent manner. You may only collect, process, and share personal data for lawful and specified purposes.

7.2 Personal data can only be processed if one or more of the following conditions apply:

7.2.1 the data subject has given their consent to the processing.
7.2.2 the processing is necessary for the performance of a contract with the data subject.
7.2.3 to meet our legal compliance obligations.
7.2.4 to protect the data subject's or another person's vital interests.
7.2.5 the processing is necessary for the performance of a task carried out in the public interest; or
7.2.6 to pursue our legitimate interests (this ground is not available to public authorities).

7.3 Additional measures apply to the processing of special category data. Two or more of the conditions set out in the UK GDPR must apply. If you are processing special category data, please contact the IGO to ensure that we are confident we are processing the data on the correct lawful basis.

7.4 Prior to processing any personal data, you must identify the legal ground that is being relied on. If you are unsure what the correct legal ground is, then please contact the IGO.

## 8. CONSENT

8.1 We may process personal data if we obtain consent to do so. A data subject consents to the processing of their personal data if they indicate agreement clearly, either by a statement or positive action, to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient methods of demonstrating consent. Explicit consent requires a very clear and specific statement (not just action).

8.2 Data subjects must easily be able to withdraw their consent at any time. Consent must be re-obtained if you intend to process personal data for a different purpose which was not disclosed when consent was first obtained.

8.3 When processing special category data or criminal convictions data, we will usually rely on a legal basis for processing rather than consent or explicit consent where possible. Where explicit consent is relied upon, you must issue a privacy notice to the data subject.

8.4 You must keep records of any consent obtained so that we can demonstrate our compliance with the UK GDPR.

## 9. TRANSPARENCY AND PRIVACY NOTICES

9.1 We must provide specific information to data subjects through privacy notices. Privacy notices must be concise, easily accessible and in clear and plain language.

9.2 Whenever we collect personal data directly from data subjects, including data collected for HR or employment purposes, we must tell them who the data controller and the Director of Resources and how and why we will use, process, disclose, protect, and retain their personal data.

9.3 When personal data is collected indirectly (for example, from a third party or publicly available source) we must provide the data subject with a privacy notice as soon as possible after collecting or receiving the data. We must also check that the personal data was collected by the third party in accordance with the UK GDPR.

9.4 If you are collecting personal data, directly or indirectly, then you must provide a privacy notice to the data subjects. For assistance with this requirement please contact the IGO.

## 10. PURPOSE LIMITATION

10.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner which is incompatible with those purposes. You cannot process personal data for any new or different purposes; you must only process it in accordance with the purpose it was originally collected for.

## 11. DATA MINIMISATION

11.1 Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. You may only process personal data when the performance of your role requires it. You cannot process personal data for any reason unrelated to your role. When personal data is no longer needed for the specified purposes, it was collected for, then it must be deleted or anonymised in accordance with our data retention policy.

## 12. ACCURACY

12.1 You must ensure that the personal data we hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

## 13. STORING PERSONAL DATA

13.1 You must not keep personal data for longer than needed in accordance with the purpose for which it was originally collected. Please refer to the Data Retention guidelines policy for further information on how long different types of personal data can be maintained for.

13.2 You must take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with our record retention guidelines. This includes requiring third parties to delete that data where applicable. The period for which we store the personal data for must be set out in the applicable privacy notice.

## 14. SECURITY, INTEGRITY, AND CONFIDENTIALITY

14.1 Personal data must be kept secure by appropriate technical and organisational measures to prevent unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

14.2 We have and will continue to develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and other identified risks. You are responsible for protecting any personal data that you process as part of your role from loss and unauthorised access, use or disclosure. You must follow all procedures we put in place to maintain the security of personal data.

14.3 You must maintain data security by protecting the confidentiality (only people who have a need to know are authorised to use the personal data can access it), integrity (personal data is accurate and suitable for the purpose for which it is processed) and availability (authorised users are able to access the personal data when they need it for authorised purposes) of personal data.

## 15. TRANSFERRING PERSONAL DATA OUTSIDE OF THE UK

15.1 The UK GDPR restricts data transfers to countries outside of the UK unless adequate measures of protection are in place. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

15.2 You may only transfer personal data outside the UK if certain conditions apply. If you believe that you, one of our suppliers or another third party engaged by us, needs to transfer our personal data outside of the UK, then you must notify the DPO prior to any transfer taking place.

## 16. DATA SUBJECT'S RIGHTS AND REQUESTS

16.1 Data subjects have rights when it comes to how we handle their personal data. These include rights to:

16.1.1 withdraw consent to processing at any time.
16.1.2 request access to their personal data that we hold.
16.1.3 prevent our use of their personal data for direct marketing purposes.
16.1.4 ask us to erase personal data if it is no longer necessary in relation to the purposes

for which it was collected or processed or to rectify inaccurate data.

16.1.5 request a copy of an agreement under which personal data is transferred outside of the UK

16.1.6 object to decisions based solely on automated processing, including profiling.

16.1.7 prevent processing that is likely to cause damage or distress to the data subject or anyone else.

16.1.8 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.

16.1.9 make a complaint to the supervisory authority (ICO); and

16.1.10 in limited circumstances, receive or ask for their personal data to be transferred to a third-party.

16.2 We must verify the identity of an individual requesting data under any of the rights listed above.

## 17. SUBJECT ACCESS REQUESTS

17.1 Data subjects have the right to receive a copy of the personal data that we hold about them. Upon receipt of a valid request and verification of the relevant identification documents, we will provide a statement confirming what personal data we hold, process, the reasons for the processing it and how long we will store it for.

17.2 All requests should be submitted to the IGO and to Dataprotection@cornwallhousing.org.uk please follow the CHL Subject Access Request Guidance (copy of guidance to be inserted here). We will respond promptly and in any one event within one month of receiving the request. Before responding we will check the identity of the person making the request.

17.3 In some cases, for example where we process large amounts of an individual's data, we may respond in a period longer than one month. We will write to the individual within one month of receiving the original request to advise them if this is the case.

## 18. FREEDOM OF INFORMATION ACT 2000 and ENVIRONMENTAL INFORMATION REGULATIONS 2004

18.1 The Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR) allows members of the public to request information from public authorities. As we are wholly owned by Cornwall Council, we may be required to provide certain information. If you receive a request under either the FOIA or EIR then you must refer it to the IGO and to housingfoi@cornwallhousing.org.uk and follow the CHL Freedom of Information Request Guidance (a link to the guidance will be inserted here)

## 19. STAFF TRAINING AND GUIDANCE

19.1 Everyone who works for or on behalf of Cornwall Housing Ltd has a responsibility for ensuring that data is collected, stored, and processed appropriately in line with the UK GDPR and this policy.

19.2 You must undergo all mandatory data privacy related training that you are directed to complete regarding compliance with data privacy laws. All staff are required to complete a

mandatory e-learning module on the UK GDPR.

19.3 Failure to comply with this policy and the UK GDPR can amount to a disciplinary offence and will be addressed under our Disciplinary Policy.

## 20. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

20.1 We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner. This means we are required to consider our data processing activities at the outset of any programme, system, or process.

20.2 The purpose of a DPIA is to systematically analyse, identify and minimise any data protection risks in a project or plan. We must conduct DPIAs in respect of any high-risk processing. This could be, for example, where you are required to process special category personal data on a large scale.

20.3 We must also conduct a DPIA when implementing major new business systems or business change programs involving the processing of personal data such any high risk-processing (such as processing special category data on a large scale), the use of new or changing technology or where automated processing (including profiling) is used.

20.4 A DPIA should include:

20.4.1 a description of the data processing and the purposes of the processing.
20.4.2 an assessment of the risk to individuals; and
20.4.3 the measures that are in place to, or are proposed to be put in place, to mitigate against any data breaches.

20.5 If you are unsure whether a DPIA is required or require further guidance on how to conduct a DPIA then please contact the IGO.

## 21. DIRECT MARKETING

21.1 Consent is required for electronic direct marketing. The limited exception for existing customers known as “soft opt in” allows an organisation to send marketing texts and email in certain limited circumstances. Data subjects can opt out of direct marketing. If you wish to use direct marketing, then please contact the IGO for further advice and guidance.

## 22. SHARING PERSONAL DATA

22.1 Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 You may only share the personal data we hold with another CHL employee if the recipient has a job-related need to know the information.

22.3 You may only share the personal data we hold with third parties, such as our service providers, if:

22.3.1 they have a need to know the information for the purposes of providing the contracted services.

22.3.2 sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained.

22.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

22.3.4 the transfer complies with any applicable cross-border transfer restrictions; and

22.3.5 a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

22.4 If you are unsure whether you are able to transfer personal data to a third-party then please contact the IGO.

## 23. DIVERSITY & INCLUSION

23.1 We are committed to treating all people with fairness and respect. We aim to create an inclusive environment where people are treated with dignity, inequalities are challenged, and we anticipate and respond positively to different needs and circumstances to enable individuals to achieve their potential and foster good relations within the communities we serve. We want to be recognised as an organisation delivering fair, inclusive, accessible services and an employer and partner of choice.

23.2 When applying this policy, we act sensitively towards the diverse needs of individuals and to reduce discrimination and harassment by making reasonable adjustments such as:

- eliminating discrimination – by providing support to tenants
- tailoring the policy to meet both the specific needs of the individual, including those with additional support needs, and the diverse needs of the wider community
- advancing equality of opportunity – treating all tenants fairly
- fostering good relationships – listening to customers and responding appropriately
- compliant with all aspects of Equality & Diversity legislation, and specifically the Equality Act 2010.

## 24. REVIEW

24.1 This policy will be regularly reviewed by the Governance and Business Support Team.

## Contact us:

Email: **info@cornwallhousing.org.uk**
Telephone: **0300 1234 161**
By letter, to **Cornwall Housing, Chy Trevail, Beacon Technology Park, Bodmin, PL31 2FR**

### Alternative formats:

If you would like this information on audio CD, audio tape, Braille, large print, any other

**Cornwall Housing Ltd, Chy Trevail,**
**Beacon Technology Park, Bodmin, PL31 2FR**

**www.cornwallhousing.org.uk**