**Section:** Finance & Resources

**Policy name: Data Protection**

**Executive responsible:** Chief Executive

**Review by:** DPO

**Tenant review:** no

**Type of review:** full

**Authority to amend:** Chief Executive

**Frequency of review:** Annually

**Last review:** May 2023

**Next review:** May 2024

**Responsibility for delivery:** Executive Team and DPO

**Supporting documents:** ICT Policy
**Data Privacy Impact Assessment (DPIA)**
**Information Asset Register (IAR)**
**Privacy Notices**
**Retention Schedule**
**Supporting Data Subject Rights Procedures**
**Breach Reporting Procedure**

**Strategy:** Business plan

**Associated risk:**
Risk 2 – failure to meet legal and regulatory requirements
Risk 4 – loss of key stakeholder support an dreputation
Risk 5 – data quality and data management is not sufficient to support the business
Risk 6 – failure to protect adequately from fraud and other crime including cyber crime

**Vfm & benchmarking:/**

| **Version control** | | | |
|---|---|---|---|
| **Version number** | **Sections amended** | **Date of update** | **Approved by** |

| | | | |
|---|---|---|---|
| 1.0 | First version in new template | June 2015 | CE |
| 2.0 | Updated for GDPR | March 2018 | CE |
| 2.1 | Updated for UKGDPR | February 2022 | DPO |
| 2.2 | Updated following internal audit recommendations | May 2023 | CE |

Introduction

This data protection policy sets out how Cornerstone Housing handle the personal data of our customers, suppliers, employees, workers and other third parties.

This data protection policy applies to all personal data Cornerstone process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

This data protection policy applies to all company personnel. Employees must read, understand and comply with this policy when processing personal data on our behalf and attend training on its requirements. This policy sets out what Cornerstone expect from employees in order for the company to comply with applicable law. Employees compliance with this policy is mandatory. Related policies and privacy guidelines are available to help employees interpret and act in accordance with this data protection policy.

The board risk appetite for legal and regulatory risks is averse. Therefore it is not acceptable to fail to meet regulations.

**Scope**

Cornerstone recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that Cornerstone take seriously at all times. The company is exposed to potential fines of up to eur20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UKGDPR and DPA 2018.

Roles and responsibilitiesThe board is ultimately responsible for ensuring that the organisation complies with laws and regulations, including data protection. They will require assurance and reporting from the DPO, executive team and auditors.

All managers are responsible for ensuring that the staff they manage comply with this data protection policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

All staff are responsible for handling data in an appropriate and secure way and ensuring that they understand their role in relation to data protection.

The DPO is responsible for overseeing this data protection policy and, as applicable, developing related policies and privacy guidelines. That post is held by Nicky Hallam, Governance Officer and DPO 01392 260532 , nicky.hallam@cornerstonehousing.net.

Please contact the DPO with any questions about the operation of this policy or the UKGDPR or if you have any concerns that this policy is not being or has not been followed. In particular, employees must always contact the DPO in the following circumstances:

- If employees are unsure of the lawful basis which they are relying on to process personal data
- If employees need to rely on consent and/or need to capture explicit consent
- If employees need to draft privacy notices or fair processing notices
- If employees are unsure about the retention period for the personal data being processed
- If employees are unsure about what security or other measures they need to implement to protect personal data
- If there has been a personal data breach
- If employees are unsure on what basis to transfer personal data outside the EEA
- If employees need any assistance dealing with any rights invoked by a data subject

- Whenever employees are engaging in a significant new, or change in, processing activity which is likely to require a DPIA or plan to use personal data for purposes others than what it was collected for;
- If employees plan to undertake any activities involving automated processing including profiling or automated decision-making
- If employees need help complying with applicable law when carrying out direct marketing activities or
- If employees need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors)

The information commissioners office (ICO) is an independent body set up to uplhold information rights. There is a wealth of information available on their website www.ico.org.uk complaints can be made via their helpline on 0303 123 1113

**Personal Data Protection Principles**

Cornerstone adhere to the principles relating to processing of personal data set out in the UKGDPR which require personal data to be:

- Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**).
- Collected only for specified, explicit and legitimate purposes (**purpose limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**data minimisation**).
- Accurate and where necessary kept up to date (**accuracy**).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**storage limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**security, integrity and confidentiality**).
- Not transferred to another country without appropriate safeguards being in place (**transfer limitation**).
- Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (**data subject's rights and requests**).

Cornerstone are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**accountability**).

## Lawfulness, Fairness, Transparency

### Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Cornerstone may only collect, process and share personal data fairly and lawfully and for specified purposes. The UKGDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that Cornerstone process personal data fairly and without adversely affecting the data subject.

The UKGDPR allows processing for specific purposes, some of which are set out below:

- The data subject has given his or her consent;
- The processing is necessary for the performance of a contract with the data subject;
- To meet our legal compliance obligations.;
- To protect the data subject's vital interests;
- To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which Cornerstone process personal data for legitimate interests need to be set out in applicable privacy notices or fair processing notices;

Employees must identify and document on the information asset register the legal ground being relied on for each processing activity.

### Consent

A data controller must only process personal data on the basis of one or more of the lawful bases set out in the UKGDPR, which include consent.

A data subject consents to 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 unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if employees

intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Where explicit consent is required, employees must issue a fair processing notice to the data subject to capture explicit consent.

Employees will need to evidence consent captured and keep records of all consents so that the company can demonstrate compliance with consent requirements.

**Transparency (notifying data subjects)**

The UKGDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate privacy notices or fair processing notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.
Whenever Cornerstone collect personal data directly from data subjects, including for human resources or employment purposes, they must provide the data subject with all the information required by the UKGDPR including the identity of the data controller and DPO, how and why Cornerstone will use, process, disclose, protect and retain that personal data through a privacy notice which must be presented when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publically available source), employees must provide the data subject with all the information required by the UKGDPR as soon as possible after collecting/receiving the data. Employees must also check that the personal data was collected by the third party in accordance with the UKGDPR and on a basis which contemplates our proposed processing of that personal data.

## Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Employees cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless employees have informed the data subject of the new purposes and they have consented where necessary.

## Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Employees may only process personal data when performing their job duties requires it. Employees cannot process personal data for any reason unrelated to their job duties.

Employees may only collect personal data that they require for their job dutiesand not excessive data. Any personal data collected must be adequate and relevant for the intended purposes.

Employees must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the company's data retention guidelines.

## Accuracy

Employees will ensure that the personal data Cornerstone use and hold is accurate, complete, kept up to date and relevant to the purpose for which Cornerstone collected it. Employees must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Employees must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

## Storage Limitation

Employees must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which Cornerstone originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The company will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.
Employees will take all reasonable steps to destroy or erase from our systems all personal data that Cornerstone no longer require in accordance with all the company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

Employees will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

## Security, Integrity and Confidentiality

### Protecting Personal Data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Cornerstone will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that Cornerstone own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). Cornerstone will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. Employees are responsible for protecting the personal data Cornerstone hold. Employees must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Employees must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.
Employees must follow all procedures and technologies Cornerstone put in place to maintain the security of all personal data from the point of collection to the point of destruction. Employees may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
Employees must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

Employees must comply with the IT policy.

### Reporting a Personal Data Breach

The UKGDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

If employees know or suspect that a personal data breach has occurred, they should not attempt to investigate the matter themselves but immediately contact the DPO. Employees should preserve all evidence relating to the potential personal data breach.

## Transfer Limitation

The UKGDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UKGDPR is not undermined.

Employees may only transfer personal data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which Cornerstone transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the UKGDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

## Data Subject's Rights And Requests

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

- Withdraw consent to processing at any time;
- Receive certain information about the data controller's processing activities;
- Request access to their personal data that Cornerstone hold;
- Prevent the use of their personal data for direct marketing purposes;
- Ask 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 or to complete incomplete data;

- Restrict processing in specific circumstances;
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the EEA;
- Object to decisions based solely on automated processing, including profiling (ADM);
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority; and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Employees must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade employees into disclosing personal data without proper authorisation).

Employees must immediately forward any data subject request they receive to the DPO.

## Accountability

The data controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The company must have adequate resources and controls in place to ensure and to document UKGDPR compliance including:

- Appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- Implementing privacy by design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of data subjects;
- Integrating data protection into internal documents including this data protection policy, related policies, privacy guidelines, privacy notices or fair processing notices;
- Regularly training company personnel on the UKGDPR, this privacy policy, related policies and privacy guidelines and data protection matters including, for example, data subject's rights, consent, legal basis, DPIA and personal data breaches. The company must maintain a record of training attendance by company personnel; and

- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

## Record Keeping

The UKGDPR requires us to keep full and accurate records of all our data processing activities.
We must keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the data controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

## Training and Audit

Cornerstone are required to ensure all company personnel have undergone adequate training to enable them to comply with data privacy laws. Cornerstone must also regularly test our systems and processes to assess compliance.

Employees must undergo all mandatory data privacy related training.

Employees must regularly review all the systems and processes under their control to ensure they comply with this data protection policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

## Privacy by Design and Data Protection Impact Assessment (DPIA)

Cornerstone 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, to ensure compliance with data privacy principles.

Employees must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

- The state of the art;

- The cost of implementation;
- The nature, scope, context and purposes of processing; and
- The risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Data controllers must also conduct DPIAs in respect to high risk processing.
Employees should conduct a DPIA (and discuss their findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling and ADM;
- Large scale processing of sensitive data; and
- Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the processing, its purposes and the data controller's legitimate interests if appropriate;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

## Automated Processing (Including Profiling) And Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- A data subject has explicitly consented;
- The processing is authorised by law; or
- The processing is necessary for the performance of or entering into a contract.

If a decision is to be based solely on automated processing (including profiling), then data subjects must be informed when employees first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

Cornerstone must also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.
A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

## Direct Marketing

Cornerstone are subject to certain rules and privacy laws when marketing to our customers.
For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

## Sharing Personal Data

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

Employees may only share the personal data Cornerstone hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
Employees may only share the personal data Cornerstone hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services;
- 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;

- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains UKGDPR approved third party clauses has been obtained.

**Acknowledgement Of Receipt And Review**

I, [employee name], acknowledge that on [date], I received and read a copy of the Cornerstone data protection policy, dated [edition date]] and understand that I am responsible for knowing and abiding by its terms. This data protection policy does not set terms or conditions of employment or form part of an employment contract.
Signed ……..
Printed name ……
Date ……

**definitions:**

**Automated decision-making (ADM)**: when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The UKGDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

**Automated processing**: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance

at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

**Company name**: Cornerstone Housing Limited.

**Company personnel**: all employees, workers [contractors, agency workers, consultants,] directors, members and others.

**Consent**: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

**Data controller**: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the UKGDPR. Cornerstone are the data controller of all personal data relating to our company personnel and personal data used in our business for our own commercial purposes.

**Data subject**: a living, identified or identifiable individual about whom Cornerstone hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

**Data privacy impact assessment (DPIA)**: tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.

**Data protection officer (DPO)**: the person required to be appointed in specific circumstances under the UKGDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the company data privacy team with responsibility for data protection compliance.

**EEA**: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit consent**: consent which requires a very clear and specific statement (that is, not just action).

**General data protection regulation (UKGDPR)**: the general data protection regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the UKGDPR.

**Personal data**: any information identifying a data subject or information relating to a data subject that Cornerstone can identify (directly or indirectly) from that data alone or in combination with other identifiers Cornerstone possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised 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.

**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 Cornerstone 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 by design**: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UKGDPR.

**Privacy notices (also referred to as fair processing notices) or privacy policies**: separate notices setting out information that may be provided to data subjects when the company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.

**Processing or process**: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

**Pseudonymisation or pseudonymised**: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

**Sensitive personal data**: information revealing 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, and personal data relating to criminal offences and convictions.