Group Data Protection Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Director of People & Governance
Author:	Governance Manager
Version number:	2.1
Approved by Executive Management Team on:	September 2021
Governing Body Approved:	15 May 2018
Effective from:	September 2021
Updated:	December 2022
Due for review on:	December 2025
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	N/A
Procedure implemented:	Yes
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	Yes
Training Completed:	Yes
Posted on intranet:	Yes
Posted on website:	Yes
Publicity material issued:	Yes
Business Services – Implementation Review:	N/A

This document can also be provided in large print, braille, audio or other non-written format, and in a variety of languages.

1. Introduction

1.1 This is the Data Protection Policy of the Caledonia Housing Association Group ("the Group"), comprising Caledonia and Cordale Housing Associations.

1.2 The policy aims to provide a general understanding of the Group's obligations under the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 and all other applicable data protection laws ("the data protection laws"). It outlines where responsibility lies for complying with the legal duties of the Group companies under the data protection laws; and the general approach the Group will take to fulfilling these duties.

1.3 Failure to comply with data protection laws could lead to financial penalties, regulatory action, disciplinary proceedings, aswell as reputational damage.

2. Scope of the Policy

2.1 The Policy applies to all personal data that the Group holds relating to living identifiable individuals ("data subjects") regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual.

2.2 The policy applies to personal data held or accessed on the Group premises or accessed remotely via remote or mobile working. Personal data stored on any removable devices is also covered by this policy.

2.3 This policy applies to:

- Governing Body Members
- Staff, including temporary staff
- Volunteers
- All contractors and suppliers working on behalf of the Group

3. Policy Statement

3.1 The Group is committed to conducting its business in accordance with all applicable data protection laws and ensuring compliance is underpinned by the principles for lawful processing of data.

3.2 Personal data must be:

3.2.1 processed lawfully, fairly and in a transparent manner in relation to data subjects;

3.2.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.2.3 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;

3.2.4 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals;

3.2.5 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.3 In addition to these principles the data protection laws require the Group to be both responsible for and be able to demonstrate compliance with the above principles.

4. Responsibilities

4.1 Policy Lead

The Director of People and Governance ("DoPG") has lead management responsibility for data protection within the Group. This will include ensuring effective implementation and regular review of this Policy; and monitoring and reporting performance against relevant compliance measures

4.2 Executive Management Team (EMT)

EMT members are responsible for ensuring the requirements of this Policy are adhered to within their respective Directorate. This will include but not be limited to:

- ensuring staff are aware of this Policy, and the associated processes and procedures;
- ensuring any requests for assistance in locating and retrieving information held by their Directorate, or teams therein, are complied with in line with required timescales.

EMT members may also be asked to undertake management checks of responses to requests; and to undertake decision reviews where appeals are

received.

4.3 Governance Team

The Governance Team, comprising the Governance Manager and Governance Officers are responsible for fulfilling the operational requirements of this Policy on a day to day basis.

This will include:

- receiving requests for information from external sources, or which have been forwarded internally, via the DP mailbox;
- providing advice to staff throughout the Group to ensure the correct identification and appropriate handling of requests for information under the UK GDPR and any other applicable data protection laws;
- logging requests for information and co-ordinating all aspects of the request handling process, including collating information and drafting and issuing responses to requesters, in consultation with relevant teams and departments;
- logging and co-ordinating Data Breaches and liaising with the Data Protection Officer (DPO) in relation to these;
- logging requests from data subjects relating to rectifying and co-ordinating all aspects of the request handling process in consultation with relevant teams and departments;
- rectifying or erasing data as requested;
- maintaining relevant registers and compiling and submitting all required performance reports;
- maintaining the Group Privacy Notice and ensuring this is made available via our public websites;
- maintaining the Privacy statement for employees and Governing Body members and ensuring these are made available via the intranet;
- assisting in the completion of Privacy Impact Assessments as required;
- maintaining the Group's Information Assets Register;
- maintaining the Group's Assets Register, and;
- maintaining records of the Group's data processing activities.

4.4 Data Protection Officer (DPO)

The Group acknowledges the requirement to appoint a Data Protection Officer (DPO) who is responsible for monitoring compliance with the UK GDPR and other data protection laws. The Group's DPO is Harper MacLeod.

The role of the DPO will include:

- ensuring compliance with the UK GDPR and all other data protection laws;
- monitoring compliance;
- providing advice and information to the Group;
- providing direct support and advice to data subjects;
- managing security incidents and breach investigations; and

- liaising with the ICO on behalf of the Group.

4.5 All employees

All employees are responsible for:

- familiarising themselves with this policy and the associated processes and procedures;
- undertaking training as required on the UK GDPR (and other applicable data protection laws), and the associated policies, processes and procedures;
- identifying information requests as such and handling any requests received in accordance with the Group's Data Protection procedures;
- seeking guidance on the identification of requests, this policy and the associated processes and procedures, or any of the duties placed on the Group by the data protection laws, from the Governance Team as and when required; and
- taking all reasonable precautions and steps to safeguard personal data in line with the data protection laws and following the data protection principles.

Any employee may be asked to assist in locating and retrieving information required as part of a response to a request.

Employees should be aware that where an information request is received and an employee deletes or alters information held by the Group, with the intention of preventing disclosure of that information, a criminal offence is committed. Where employees are unsure if deletion or alteration of information may result in an offence they should seek guidance from the Governance Team in the first instance.

Compliance with this policy is compulsory for all Group employees. Any employee who fails to comply with this policy may be subject to disciplinary action.

5. Processing Lawfully and Fairly

5.1 The Group will ensure processing of personal data only takes place where one of the following criteria ("lawful basis") are met:

1. that the data subject has consented to the processing;
2. that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. that the processing is necessary for compliance with a legal obligation to which the Group is subject;
4. that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
5. that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

6. that the processing is necessary for the purposes of legitimate interests of the Group or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

Where the Group requires to process sensitive data relating to a data subject's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) or information concerning a data subject's health, sex life or sexual orientation ("special category data"), in addition to meeting one of the above lawful basis, it will also meet one of the following conditions:

1. the data subject has given explicit consent;
2. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Group or the data subject;
3. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
4. processing relates to personal data which are manifestly made public by the data subject;
5. the processing is necessary for the establishment, exercise or defence of legal claims; or
6. the processing is necessary for reasons of substantial public interest.

Data subjects will be advised on the purpose and legal basis for processing, and all other information the Group is required to provide via a freely available Privacy Notice Privacy Notices will be provided to data subjects from the outset of processing.

5.2 Where data subjects' consent is required to process personal data, this consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

6. Carrying out Assessments

6.1 Where processing is carried out on the basis of a legitimate interest, a legitimate interest assessment will be conducted to ensure due regard is given to the interests of the data subject. A record will be kept of any assessments made.

6.2 Where any processing is likely to result in a high risk to a data subject's rights, a data protection impact assessment will be conducted prior to processing taking place. Such assessment will assess:

- whether processing is necessary and proportionate;
- the potential risks to the data subject; and
- what measures can be put in place to address those risks.

A record will be kept of any assessments made and will be recorded by the Governance Team

7. Purposes for Processing

7.1 Personal data will only be used for the original purpose it was collected for. These purposes will be made clear to all data subjects.

7.2 If the Group wish to use personal data for a different purpose than previously notified, we will notify the data subject prior to processing.

8. Criminal data processing

8.1 Where the Group identifies a requirement to process criminal record data as part of any recruitment process, it will ensure that:

- the criminal record data requested is limited only to offences that have a direct bearing on the role applied for;
- it is only obtained following a conditional offer;
- it only retains the criminal record data for as long as is necessary to make a determination on whether to proceed with the offer (but may retain a record that a determination was made); and
- a fair determination will be made in all circumstances, taking account of the relevance, seriousness, circumstances, age of offence and any other relevant factors.

9. Adequate and Relevant Data

9.1 The Group will only collect the minimum personal data required for a specified purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted.

9.2 Any personal information that is optional for data subjects to provide will be clearly marked as such.

10. Accuracy of Data

10.1 The Group will take appropriate steps to keep personal data up to date, where relevant, to ensure accuracy and correct processing.

10.2 Any personal data found to be inaccurate will be updated without undue delay and within one month of receipt.

10.3 Any inaccurate personal data that has been shared with third parties will also be updated.

11. Retention

11.1 The Group will hold data for the minimum time necessary to fulfil its purpose and will notify data subjects of this via the relevant Privacy Notice. Timescales for the retention of personal data will be outlined in the Group's Records Retention Schedule

11.2 Data will be disposed of in a responsible way to ensure confidentiality and in line with Group Information and Destruction Policy.

12. Security

12.1 The Group will implement appropriate security measures to protect personal data in line with the Group Information Security Policy, including ensuring the availability and access to personal data can be maintained or restored following any incident.

12.2 Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis.

12.3 Employees will keep all data secure, by taking all reasonable precautions and practical steps following the Group Information Security Policy.

13. Data Sharing

13.1 In certain circumstances the Group will share personal data with third parties. This may be part of a regular exchange of data, data sharing from one part of the organisation to another or one-off disclosures in unexpected or emergency situations.

13.2 Appropriate security and technical measures will be used when sharing any personal data to ensure no unauthorised access to the data. Security measures will be appropriate to the nature / scope / context and purpose of the processing and will be assessed on a case-by-case basis and will include but not limited to encryption and passwords.

13.3 Where data is shared with a third party a contract or data sharing agreement will be in place to establish what data will be shared, the agreed purpose and in all cases only share what is required for the stated purpose. Where the third party processes data on behalf of the Group ("data processor") the Group will retain overall responsibility for that data and the data processor contract will contain the relevant provisions required by law.

13.4 The Group will consider all the legal implications of sharing personal data prior to doing so.

13.5 Data Subjects will be advised of any data sharing in the Privacy Notice.

13.6 When sharing personal data, the Group may transfer personal data outside the UK and/or to international organisations on the basis that that country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses included in a signed contract in accordance with paragraph 13.3.

14. Right of Access - Subject Access Requests

14.1 Data subjects have the right to access their personal data, and this applies to every individual who we obtain and process personal data about. This is referred to as a Subject Access Request:

- The Group will respond to all information requests promptly and in any event within one calendar month. It acknowledges that this can be extended up to three months should the request be complex in line with the legal requirements and detailed guidance in our procedures.

- We cannot refuse to respond to a request in most circumstances.

- There is no fee for carrying out this request in most circumstances.

- The Group may obtain advice from the DPO where requests are particularly complex.

15. The Right of erasure (to be forgotten)

15.1 Data subjects can exercise their right to "be forgotten" by submitting a request to the Group seeking that the Group delete all the data subject's personal data. However, this right is not absolute, and the right applies when:

- that personal data is no longer necessary;
- where applicable, the individual withdraws their consent;
- the data subject objects to the processing and the Group has no grounds to refuse that objection;
- the personal data has been unlawfully processed; or
- the Group is legally obliged to delete the personal data

15.2 Each request received by the Group will be considered on its own merits. After reaching a decision the Group will respond in writing to the request.

16. The Right to Restrict or Object to Processing

16.1 Data subjects may request that the Group restrict its processing of personal data, or object to the processing of that data. This is likely to apply where there is any dispute over the accuracy or lawfulness of the processing.

16.2 In the event that any direct marketing is undertaken from time to time by the Group, an individual has an absolute right to object to this marketing and if the Group receives a written request to cease direct marketing, then it will do so immediately.

16.3 Each request received by the Group will require to be considered on its own merits.

17. Right to be Informed

17.1 Subjects have a right to the information provided in Privacy Notices which details how their data is processed. This includes personal data collected directly from the subjects or from another source.

18. Right to Rectification

18.1 Where personal data is found to be inaccurate or incorrect, the Group must comply with any request to rectify that data.

19. Right to Data Portability

19.1 Where the lawful basis for processing is consent or contract and the processing is by automated means (i.e. electronic and not hardcopy files), a data subject may instruct the Group to transfer the personal data it processes to another data controller in a format that is structured, commonly used and machine-readable for use by the other controller. Specifically, this right does not apply to any data processed in the public interest or as part of a legal obligation.

20. Security Incident and Breach Management

20.1 A personal data breach is any event in which there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All breaches must be reported whether caused by any internal or external event or person.

20.2 All security incidents or personal data breaches must be reported to and subsequently investigated and managed by the Governance Team and the Data Protection Officer in conjunction with the IT Systems Manager where appropriate and in line with the Group Information Security Policy and the Group Security Incident and Breach Management Procedures.

20.3 The Information Commissioner's Office, the individuals affected and any relevant third parties will be notified immediately, if required. The Group Data Protection Procedures outlines the circumstances under which it may be appropriate to notify the individuals and where required the advice of the DPO will be sought in regards to this.

20.4 A record of all data breaches, whether reportable or not, will be maintained.

21. CCTV and Surveillance Systems

21.1 The Group owns and operates CCTV and other forms of surveillance systems at various premises, including offices, residential properties and community facilities, and in work vehicles. We do this for the purpose of enhancing security where we consider there to be a risk of crime or a potential threat to the health, safety and wellbeing of individuals; and to assist in the prevention and detection of criminal or anti-social behaviour

21.2 The Group acknowledges the obligations it incurs in operating such systems and the rights and freedoms of those whose images may be captured. We are committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulation (the UK GDPR) and UK Data Protection Act 2018 (the DPA 2018).

21.3 The Group will maintain and adhere to strict procedures governing the installation, operation, use and decommissioning of CCTV systems. As part of this it will maintain:

- A register of all systems installed, capturing relevant information including address and purpose of the installation, installation dates and review details, technical specifications, and location of cameras, equipment and signage.
- A record of all Data Protection Impact Assessments (DPIA) carried out as part of the installation decision making process, including details of relevant consultation activities
- A register of all requests for disclosure of CCTV images, including details of the individual(s) or agency making the request, the purpose of the request and the decision to disclose or withhold images.

22. Training

22.1 Appropriate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities

22.2 All staff, volunteers, and Governing Body members will be made aware of good practice in Data Protection and where to find guidance and support for data protection issues.

23. Related Policies and Procedures

23.1 This policy is an essential component of the Group's Information Risk Management practices. Please refer to the Group Information Risk Management policies for details on related policies and procedures.

24. Policy Review

24.1 This policy shall be subject to review every three years, or sooner if required by legislative or other change.

25. Compliance Statement

25.1 It is important that all members of staff, in carrying out their duties for the Group, do so in accordance with the Group's policy framework. Our policy framework ensures we comply with laws and regulation, while giving guidance to inform operations and decision-making. Our policies have been designed to be clear and easy to understand, and are available on our website and intranet. If any member of staff is unclear as to their responsibilities under this policy, then they should refer to their line manager and / or the policy author for further guidance. A failure to comply with Group policies can have serious consequences for the Group. Should an employee become concerned about serious non-compliance with the policy, they should speak to their line manager or refer to the guidance set out in the Group Whistleblowing policy.