



Group AI Adoption and Use Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Executive Director of Finance (EDoF)
Author(s):	Head of IT / EDoF
Version number:	1.0
Approved by Chief Executive:	Yes
Approved by Group Governing Bodies:	Yes
Effective from:	1 June 2026
Due for review on:	1 June 2027
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	Yes
Procedure implemented:	N/A
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	N/A
Training Completed:	Inflight
Posted on intranet:	
Posted on website:	Yes
Publicity material issued:	N/A
Audit Committee – Implementation Review:	TBC

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

Caledonia Housing Group

Artificial Intelligence (AI) Adoption & Use Policy

Table of Contents

1. Introduction
2. Purpose
3. Scope of the Policy
4. Definitions
5. Governance and Regulatory Alignment
6. Legal and Standards Framework
7. Guiding Principles
8. Roles and Responsibilities
9. Approved Tools and Data Classification
10. Acceptable Use & Good Practice
11. Use of Artificial Intelligence (AI) in Employment
12. Race and Language Considerations
13. Disability and Accessibility
14. Human Oversight and Equality Compliance
15. Procurement, Third Parties & Contracts
16. Tenant and Stakeholder Engagement
17. Training and Awareness
18. Risk Management, Assurance & Audit
19. Incident Management
20. Monitoring, Review and Policy Maintenance
21. Compliance Statement
22. Appendix A: Data Classification Matrix

1. Introduction

1.1. The goal of the use of artificial intelligence (AI) within the Caledonia Housing Group (“the Group”) is to achieve efficiencies in terms of improved business operations, reduced operational costs and enhanced tenant service in alignment with the five-year business plan and compliance with the related laws and regulations.

2. Purpose

2.1. The purpose of this Policy is to enable safe, ethical and value adding adoption of AI across the Group, improving tenant services, organisational efficiency and staff productivity while maintaining compliance with Scottish RSL regulatory requirements, data protection law and recognised good practice.

2.2. This Policy supports the SHR Regulatory Framework and our internal self-assurance and governance arrangements.

3. Scope of the Policy

3.1. This Policy applies to all Group employees, temporary staff, contractors, Board/Governing Body members and third-party providers who procure, configure or use AI systems for or on behalf of the Group.

3.2. It covers all AI use across tenant services, asset management, repairs & maintenance, finance, HR, communications and back-office functions, regardless of whether AI is embedded in existing systems or accessed as standalone tools.

4. Definitions

4.1. **Artificial Intelligence (AI):** Systems that autonomously or semi autonomously process data to make predictions, recommendations, or decisions (including generative AI), noted for features such as adaptivity and varying degrees of autonomy.

4.2. **Caledonia Housing Group:** Referred to as the ‘Group’ in this document, comprises Caledonia Housing Association and Cordale Housing Association.

4.3. **DPIA:** Data Protection Impact Assessment

4.4. **Generative AI:** AI that produces new content (text, images, audio, code) based on patterns learned from data.

4.5. **High-risk AI use (Group context):** Any AI use that is likely to significantly affect individuals’ rights or outcomes (e.g., access to housing or services), process special category data at scale, or involve automated decision-making with legal/similarly significant effects.

4.6. Significant decisions impacting employees include decisions that materially affect an employee's employment, opportunities, terms and conditions, or wellbeing, such as (but not limited to) recruitment, performance management, promotion, flexible working, attendance management, or conduct.

4.7. Significant decisions impacting customers are decisions that materially affect a person's housing, tenancy, access to services, financial obligations, safety, or legal rights, such as (but not limited to) housing allocation decisions, tenancy-related decisions, arrears and recovery action, complaints outcomes, and decisions relating to repairs or access to support services).

4.8. **Human Oversight of AI:** Ensuring appropriately trained employees remain responsible for reviewing, validating and approving AI-generated outputs.

5. Governance and Regulatory Alignment

5.1. The Group will incorporate AI governance into its established assurance processes, Board oversight, and organisational risk management framework. This will align with the requirements of the Scottish Housing Regulator's Regulatory Framework and SFHA self-assurance expectations, including documenting AI use within assurance evidence, updating relevant risk registers, and providing Board reporting on significant AI deployments and associated risks.

5.2. The Group will align with the Scottish Governments' AI Strategy ethos, trustworthy, ethical and inclusive, and consider the Scottish AI Playbook resources as they evolve.

5.3. We will follow the UK's pro-innovation, principles-based approach to AI regulation (safety, transparency, fairness, accountability, contestability), implemented through existing regulators.

5.4. All new Artificial Intelligence (AI) and AI-enabled systems, solutions, tools, or significant enhancements shall be subject to review and approval by the Change Assurance Committee (CAC) prior to procurement, implementation, or deployment. As part of its assessment, the Committee will consider:

- The business need, expected benefits, and strategic value of the proposed AI solution.
- Compliance with applicable legislation, including data protection, information security, equality, human rights, and housing sector regulatory requirements.
- Risks associated with the use of AI, including privacy, security, bias, transparency, explainability, accuracy, and operational resilience.

- The potential impact on tenants, customers, employees, and other stakeholders.
- Financial implications, including acquisition, implementation, ongoing support, licensing, and long-term costs.
- Governance arrangements, accountability, and appropriate human oversight of AI-driven decisions or recommendations.
- Requirements for monitoring, performance measurement, auditability, and ongoing assurance throughout the lifecycle of the AI system

5.5. The Change Assurance Committee may approve, reject, or require further review of any AI-related proposal and may escalate significant risks or strategic considerations to the Executive Management Team (EMT) where appropriate. No AI solution shall be implemented without documented approval through the organisation's established governance processes.

5.6. The Committee will also oversee the ongoing assurance of deployed AI systems, ensuring that they continue to operate safely, effectively, ethically, and in compliance with organisational policies and regulatory requirements.

6. Legal and Standards Framework

6.1. All AI uses that process personal data must comply with lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality and accountability requirements.

6.2. Where AI materially influences decisions or communications with tenants/staff, the Group will provide clear and accessible information about the role of AI and, where applicable, meaningful information about the logic and its significance.

6.3. The Group will avoid solely automated decisions ensuring there is appropriate human oversight of all AI generated output.

7. Guiding Principles



Transparency: Tenants and staff must be informed when AI is used in decision-making or communication.



Human oversight is required for all AI-generated outputs that affect tenants or staff.



Fairness & Inclusion: AI systems must not reinforce bias or discrimination.



Security & Resilience: All AI tools must comply with GDPR and the UK Data Protection Act 2018.



Value-Driven: AI should enhance—not replace—human services and decision-making.



Continuous Improvement: Leverage sector resources to share learnings & maturity

7.1. Risk based adoption: Prioritise use cases that deliver tenant and organisational benefit with manageable risk; scale only when controls are effective.

7.2. Human oversight: Ensure that appropriately trained employees remain responsible for reviewing, validating, and approving AI-generated outputs before they are used to inform decisions, actions, communications, or business processes. Human oversight requires individuals to assess the accuracy, relevance, fairness and appropriateness of AI outputs, apply professional judgement, and intervene where necessary to correct errors, challenge recommendations, or prevent unintended consequences.

AI should be used as a tool to support decision-making rather than replace it, with ultimate accountability remaining with designated employees. This is particularly important in tenant facing activities, where human review helps ensure decisions are transparent, compliant, accurate and aligned with organisational policies and values.

7.3. Fairness & inclusion: Proactively assess and mitigate bias and potential harms, engaging tenants where appropriate and ensuring accessibility.

7.4. Security & resilience: Apply robust technical and organisational measures; adopt enterprise managed solutions; minimise data exposure; monitor models for drift and misuse.

7.5. Transparency with tenants: Inform tenants when AI is used in services that affect them; provide contact routes for queries/concerns and reasonable opt-outs where feasible.

7.6. **Continuous improvement:** Leverage sector resources (e.g., SFHA AI readiness and networks) to share learning and uplift maturity.

8. Roles and Responsibilities

8.1. **Board/Audit & Risk Committee:** Oversight of AI strategy, risk, and compliance; approve AI use and review the AI Register and assurance reporting.

8.2. **Change Assurance Committee (CAC):** Will provide independent assurance that proposed AI solutions are aligned with the organisation's strategic objectives, regulatory obligations, risk appetite, and ethical standards.

8.3. **Executive Management Team:** Accountable for implementing this Policy and resourcing controls (training, DPIAs, security).

8.4. **Data Protection Officer (DPO):** Advises on DPIAs, lawful bases, transparency, data subject rights and vendor contracts.

8.5. **Head of Information Communication Technology (ICT):** Ensures secure adoption, configuration, access control, logging/monitoring, and incident response for AI tools in line with NCSC (National Cyber Security Centre) /DSIT (Department for Science, Innovation and Technology) guidance.

8.6. **All Staff and Contractors:** Use only approved tools for approved purposes; follow training; report issues immediately.

9. Approved Tools and Data Classification

Approved enterprise AI

9.1. The Group will only permit the use of enterprise-managed AI solutions that have been assessed and approved through the organisation's governance framework and meet all contractual, information security, data protection, and regulatory requirements. Approved AI solutions will be recorded in the AI Register and reported to the Executive Management Team (EMT) and Audit & Risk Committee as appropriate. Any new AI tool requires approval through the AI Use Case & Risk Assessment process and (where relevant) procurement due diligence.

Data Classification & Permitted Use

9.2. Use of AI must comply with the Data Classification Matrix (Appendix A). As a rule:

- **Public:** May be processed in approved AI tools, per the data classification matrix.
- **Internal:** May be processed only in approved enterprise AI tools configured for organisational use.

- Confidential: Personal or commercially sensitive data may be processed only in approved enterprise AI with a completed DPIA (if high-risk) and appropriate minimisation/pseudonymisation.
- Restricted (Highly Confidential / Special Category): Prohibited in AI systems unless an explicit exemption is approved by the DPO following a DPIA and additional controls; use of public/free AI for this class is forbidden.

10. Acceptable Use & Good Practice

- Treat enterprise AI as a **productivity assistant** to accelerate work, not a substitute for professional judgement.
- All AI-generated outputs must be reviewed, validated, and approved by an appropriately authorised employee before use. Under no circumstances should AI outputs be automatically implemented, actioned or incorporated into communications, decisions or processes without human oversight and approval.
- **Tone of voice:** AI-assisted content must follow the Groups Tone of Voice Guidelines. Where appropriate, colleagues can upload or reference the guidance within their prompts to help generate content that reflects the Groups communication standards.
- **Prompt hygiene:** Do not include unnecessary personal data; prefer summaries or anonymisation; avoid uploading Restricted data.
- **Recordkeeping:** For material uses, retain prompts and outputs (or summaries) in the working record where they inform decisions.

11. Use of Artificial Intelligence (AI) in Employment

- 11.1. Caledonia Housing Association recognises that Artificial Intelligence (AI) has the potential to improve efficiency, support decision-making, enhance service delivery, and reduce administrative burdens within employment-related activities.
- 11.2. AI may be used to assist with tasks such as drafting documents, summarising information, analysing data, supporting workforce planning, creating training materials, and improving the employee experience.
- 11.3. However, AI is intended to support employees in carrying out their roles and must not replace human judgement, professional expertise, or managerial accountability.
- 11.4. The use of AI in employment matters must comply with all relevant legal and regulatory requirements, including employment law, equality legislation, data protection legislation, and the expectations of the Scottish Housing Regulator.

- 11.5. AI may be used to assist recruitment and selection processes, such as drafting job descriptions, preparing interview questions, reviewing applications, or identifying potential skills gaps.
- 11.6. AI must not be used as the sole basis for employment decisions. All recruitment, appointment, promotion, disciplinary, grievance, performance management, and dismissal decisions must be reviewed and approved by an appropriately authorised manager. Human decision-makers must consider the individual circumstances of each case and remain accountable for all employment related outcomes.
- 11.7. Where AI is used in relation to employees, the Group will ensure that appropriate safeguards are in place to prevent unlawful discrimination, bias, or unfair treatment. Employees must not be subject to significant decisions based solely on automated processing. Any AI generated recommendations, assessments, or analyses must be critically reviewed by a suitably trained employee before any action is taken.
- 11.8. Significant decisions include those that materially affect an employee's employment, opportunities, terms and conditions, or wellbeing, such as (but not limited to) recruitment, performance management, promotion, flexible working, attendance management, or conduct.
- 11.9. The Association will not use AI to undertake covert monitoring or surveillance of employees. Any use of AI-enabled monitoring tools must be lawful, proportionate, transparent, and clearly communicated to employees in advance. Such monitoring must have a legitimate business purpose and comply with the Groups data protection and employee privacy obligations.
- 11.10. Per the Data Classification Matrix, managers and employees using AI tools as part of their work are responsible for ensuring that confidential, personal, commercially sensitive, or tenant-related information is not uploaded to unauthorised AI platforms. Appropriate security controls, governance arrangements, and training will be maintained to ensure the safe and responsible use of AI technologies.

12. Race and Language Considerations

- 12.1. The organisation recognises that employees, applicants and service users may have different linguistic and cultural backgrounds. The use of AI-powered translation tools carries a risk of inaccurate translation, cultural misunderstandings, or inappropriate wording which may disadvantage individuals whose first language is not English. To mitigate this risk:

- AI generated translations must not be relied upon for critical, legal, contractual, disciplinary, grievance, health and safety, or other high-risk employment communications.
- Important employment documents, including contracts of employment, policy documents, formal notifications, and documents relating to employee rights or obligations, must be translated using approved professional translation services where required.
- Employees must not make employment decisions based solely on AI-generated translations and should seek clarification where there is any uncertainty regarding meaning or context.
- Human review will be undertaken to ensure communications are accurate, culturally appropriate, and do not disadvantage individuals based on race, ethnicity, nationality, or language.

13. Disability and Accessibility

13.1. The organisation acknowledges that AI systems may not consistently produce content that is accessible to individuals with disabilities and may fail to meet accessibility standards or reasonable adjustment requirements. To mitigate this risk:

- All AI-generated content used in employment-related activities will be reviewed by a suitably trained employee before publication or use.
- Reviews will assess compliance with the organisation's accessibility requirements, inclusive communication standards, and tone of voice.
- AI-generated content must be checked to ensure compatibility with assistive technologies, where applicable, and compliance with recognised accessibility standards.
- Employees must not rely solely on AI-generated outputs when making decisions that could affect disabled employees or applicants.
- Where reasonable adjustments are required, human oversight will ensure that AI tools do not create barriers to recruitment, employment, development opportunities, or workplace participation.

14. Human Oversight and Equality Compliance

14.1. The organisation remains responsible for all decisions informed by AI systems. AI outputs must not replace human judgement in employment matters. Employees using AI tools must consider potential impacts on protected characteristics under the Equality Act 2010 and take appropriate steps to prevent discrimination, disadvantage, or exclusion. Human review and oversight will be applied proportionately to the level of risk associated with the activity being undertaken.

15. Prohibited & Restricted Uses

- 15.1. The following are prohibited unless explicitly approved through the High-risk AI route (DPIA + governance approval):
- Solely automated decisions with legal or similarly significant effects (e.g., eligibility decisions).
 - Processing Restricted/Special Category data in AI systems, except where strictly necessary, lawful, risk assessed and formally approved with enhanced control.
 - Use of public/free AI (e.g., consumer chatbots) with Internal, Confidential or Restricted data.
 - Deploying AI that cannot provide appropriate transparency/explainability for impacted individuals where required.

16. Procurement, Third Parties & Contracts

- 16.1. Due diligence: All suppliers must demonstrate compliance with UK GDPR (including roles as controller/processor), security of processing, data location/transfer terms, bias and explainability testing as applicable, and auditability.
- 16.2. Cyber requirements: Contracts should reflect secure by design expectations and alignment to the AI Cyber Security Code of Practice (and implementation guide) and relevant NCSC guidance. All AI vendors and significant AI enabled procurements must be recorded in the AI Register and supplier/contract records.

17. Tenant and Stakeholder Engagement

- 17.1. Be transparent with tenants when AI is used in ways that materially affect services; provide plain English notices and channels for questions and complaints.
- 17.2. Where practicable, build tenant voice into design and review of higher impact use cases, aligning with the sector's emphasis on openness and accountability.

18. Training and Awareness

- 18.1. Mandatory annual training for all staff on AI acceptable use, data protection and cyber security; targeted training for AI Service Owners and technical teams.
- 18.2. The Group will draw on SFHA resources (e.g., AI Readiness Tool, AI Champions Network) and sector cyber training to uplift capability.

19. Risk Management, Assurance & Audit

- 19.1. Maintain an AI Register of approved tools/use cases, risk ratings, DPIA status, supplier details and owners.
- 19.2. Conduct DPIAs and technical security reviews for medium/high-risk use; embed monitoring for accuracy, bias, drift and misuse.
- 19.3. Report AI risk and assurance through existing governance channels to support the Annual Assurance Statement and regulatory engagement.

20. Incident Management

- 20.1. Any suspected data breach, malfunction, harmful output, security incident or misuse pertaining to any AI tooling or process must be reported immediately to the IT Service Desk and DPO via the standard incident route; incidents will be handled under the Group's Information Security & Data Breach Procedures with regulatory notification where required.

21. Monitoring, Review and Policy Maintenance

- 21.1. Monitoring: The Head of ICT and DPO will monitor compliance, supported by internal audit.
- 21.2. Review: This Policy will be reviewed annually and updated sooner to reflect changes to SHR requirements, ICO guidance, or UK/Scottish AI policy

22. Compliance Statement

- 22.1 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.

Appendix A: Data Classification

Data Classification Type	1. Public	2. Internal	3. Confidential	4. Restricted (Highly Confidential)
A. Definition	<i>Information that has been approved for public release / sharing with anyone.</i>	<i>Routine business information not intended for public disclosure.</i>	<i>Personal or commercially sensitive Information that could cause material harm if disclosed.</i>	<i>Information, including Special Category Data, whose unauthorised disclosure could cause serious harm.</i>
B. Examples	Website content Press releases Approved Marketing Policies Published Reports	Team Procedures Internal Announcements Internal Meeting Notes Non-Sensitive Staff rotas Internal Project Updates	Tenant Account Details Repairs Records Basic Staff Information Vendor Contracts	Payroll bank details Tenant Personal data (health, disability, ethnicity, domestic abuse, mental health) Eviction case packs
C. Regulatory Requirement				
D. Risks if Disclosed	None to Negligible	Low (could cause minor operational disruption or reputational nuisance).	Moderate to high (financial, contractual, reputational).	Severe (legal/regulatory penalties, material financial loss, operational risk).

Data Classification Type	1. Public	2. Internal	3. Confidential	4. Restricted (Highly Confidential)
E. Access Control	Unrestricted	Staff-only	Restricted to privilege, HOS approval	Restricted to privilege, EMT approval
F. Typical AI Use Allowed	Free to use in approved public or enterprise AI.	Use in enterprise AI only. Avoid external / public models with default consumer terms	Use only in enterprise AI plus redact personal data.	Do not input into AI.
G. Output Handling	Public as needed, manual verification of accuracy.	Treat as Internal unless specifically approved for External use.	Treat as Confidential to prevent leakage of sensitive data.	n/a reference above.
H. AI Adoption - Third Party Vendors	Light Due Diligence	Due Diligence plus contracted no train clauses.	Contractual Controls including no data retention / training, sub-processor transparency, UK / EU residency, pen test . SOC2 / ISO 27001	Enhanced due diligence, Transfer Impact Assessment, first party / sovereign offerings only.