Cloch Housing Association

AI Usage

Policy Name	AI Usage (Artificial Intelligence)
Policy Category	IT
Policy Number	128
Approved by	F&CS Sub-Committee
Responsibility of	ICT Manager
Date Adopted	03/09/2024
Last Review	n/a
This Review	03/09/2024
Next Review	September 2027
Equalities Impact Assessment Required	No
Link to other policies	ICT Strategy
Consultation	No
Need for Procedure	Yes

1. Introduction

Artificial Intelligence (AI) tools are transforming the way we work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations.

However, the use of AI tools also presents new challenges in terms of information security and data protection. This policy is a guide for employees on how to be safe and secure when using AI tools, especially when it involves the sharing of potentially sensitive company and customer information.

2. Purpose

The purpose of this policy is to:

- outline best practices for the use of artificial intelligence tools within the workplace, especially as it pertains to using sensitive data and proprietary company and customer information in these tools; and
- ensure that all employees use AI tools in a secure, responsible and confidential manner.

The policy outlines the requirements that Cloch Housing Association employees must follow when using AI tools, including the evaluation of security risks and the protection of personal and confidential data.

3. Policy statement

Cloch Housing Association recognises that the use of AI tools can pose risks to our operations and customers. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all company and customer data. This policy requires all employees to use AI tools in a manner consistent with our data protection and security best practices.

4. Compliance with Laws and Regulations

AI systems must be used in compliance with all applicable laws and regulations, including data protection, privacy, intellectual property laws, copyright and trade secrets.

5. Data Protection and Security Requirements

All Cloch Housing Association employees must adhere to the following data protection and security requirements which are considered best practice when using AI tools:

- Evaluation of AI tools: The organisation must evaluate the security of any AI tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. Pose questions such as 'Does the system provider perform penetration testing and security audits', or 'Does the system provide end-end encryption?'. AI tools may also release what is known as a 'model card' or 'system card', which documents information relating to the systems' safety implementations and concerns, potential limitations, and evaluation data. The organisation must also check the reputation of the tool developer and any third-party services used by the tool. Ultimately, it is the responsibility of management to approve the usage of any AI tools for standard business usage, and these should be added to a register of approved AI products. Before using or approving an AI product for organisational usage, it may be beneficial to carry out a DPIA in order to understand potential risks.

- Protection of personal and confidential data: Employees must not upload or share any data that is personal, confidential, proprietary, or protected by regulation within the AI system. This includes data related to customers, clients, employees, or other third parties, and in particular, information that a) can identify any of the above-mentioned individuals, b) is considered sensitive in it's nature, or c) is personal or special category personal data as defined under Articles 4 and 9 of UK GDPR.
  Be mindful of whether it is possible to indirectly identify an individual from the content you enter into the system, i.e. asking AI to write a Job description which relates to a position held by only one person.
  If you intend to process personal data using an AI product, then it is recommended that you carry out a DPIA.

- Access control: Employees must not give access to AI tools outside the organisation without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties. Any work-related access to AI systems should be solely maintained through corporate managed accounts, rather than individual's own personal access to the system.

- Use of reputable AI tools: The organisation should use only reputable AI tools and be cautious when using tools developed by individuals or companies without established reputations. Any AI tool used by employees must meet our security and data protection standards. Where deemed necessary, a data processing agreement with the system provider may be executed.

- Compliance with security policies: Employees must apply the same security best practices we use for all organisation and customer data. This includes using strong passwords, keeping software up-to-date, use of multi-factor authentication, and following our data retention and disposal policies.

- Use of organisational data: Employees must reject the use of our organisation's data for the AI's training purposes, save where approval has been granted by senior management. Where possible, employees must utilise any opt-out functionality to ensure data is not used for the improvement of any large-language models or non-API services.

- Bias and Fairness: AI Systems unavoidably make biased decisions. Employees must actively work to identify biases in the output of AI systems. They should ensure that content generated as a result of using these systems is fair, inclusive, and does not discriminate against any individuals or groups. All AI system outputs must be checked for any possible discrimination.

- Data Protection: Employees must exercise caution when sharing information publicly. As a first step, employees must ask themselves the question, "Would I be comfortable sharing this information outside of our organisation? Would we be okay with this information being leaked publicly?" before uploading or sharing any data into AI tools.
  The second step is to follow the second bullet point above in relation to the protection of personal and confidential data.

- Hallucinations: Hallucinations are the production of content that is nonsensical or untruthful in relation to certain sources. This tendency can be particularly harmful as AI systems become increasingly convincing and believable, leading to overreliance on them by users. Counterintuitively, hallucinations can become more dangerous as systems become more truthful, as users build trust in the system when it provides truthful information in areas where they have some familiarity. Employees must therefore ensure they review each output from AI systems, and where required, verify the accuracy against additional non-AI resources.

Hallucinations can be reduced through following core competencies when prompting AI, such as avoiding ambiguity and vagueness, avoiding misuse of terminology, and avoiding merging of unrelated concepts.

6. Human-AI Collaboration

Cloch Housing Association employees should recognise the limitations of AI and always use their judgement when interpreting and acting on AI-generated recommendations. AI systems should be used as a tool to augment human decision-making, not to replace it.

Any decision with legal effect must be made by humans.

7. Review and revision

This policy will be reviewed and updated on a 3-yearly basis or as needed based on the evolution of AI technology and the regulatory landscape to ensure that it remains current and effective. Any revisions to the policy will be communicated to all employees.