
CK Asset Holdings Limited

Responsible Use of GenAI Policy

CKA Responsible Use of GenAI Policy

This Responsible Use of GenAI Policy (this “**Policy**”) has been developed by CK Asset Holdings Limited (the “**Company**”) for the Company and its subsidiaries (collectively the “**Group**”).

1. Introduction

- (a) Generative Artificial Intelligence (“**GenAI**”) refers to artificial intelligence systems, models, tools and applications that can generate, analyse, transform or otherwise produce text, images, audio, video, code, data, recommendations or other outputs in response to user prompts, instructions or other inputs. For the purposes of this Policy, references to GenAI also include AI assistants and AI agents that can retrieve information, generate content, perform tasks or initiate actions on behalf of users.
- (b) The Group recognises that GenAI has the potential to enhance productivity, innovation and operational efficiency, and support the delivery of high-quality work. As GenAI capabilities continue to evolve, appropriate governance, human oversight and controls are essential to ensuring that GenAI is used in a secure, ethical, responsible and lawful manner.
- (c) The purpose of this Policy is to promote the responsible use of GenAI tools by employees for work-related purposes or on devices provided by the Group while managing the associated risks. If any provisions set out in this Policy are inconsistent or in conflict with any such law, rules or regulations, such law, rules or regulations will prevail to the extent of such inconsistency or conflict.
- (d) Employees may only use GenAI tools that have been approved by the IT Department and listed on the Company’s intranet from time to time (“**Permitted GenAI Tools**”) for work-related purposes or on devices provided by the Group. No other GenAI tools may be used for work-related purposes or on devices provided by the Group without prior written permission from the IT Department.
- (e) All Company employees (whether full time or part time, contract or temporary staff, or interns) are required to comply with this Policy. The Company’s overseas subsidiaries and joint ventures over which the Group has management control shall adopt and maintain GenAI use policies that are in compliance with the law, rules and regulations of the jurisdictions in which they operate and are consistent with the principles set out in this Policy. The Company may require its consultants, secondees, advisors and other persons with access to the Group’s information or systems to comply with this Policy.
- (f) This Policy must be read in conjunction with other relevant policies and procedures of the Company. Any technical questions in relation to this Policy should be directed to the IT Department (aisupport@ckah.com). Any legal questions in relation to this Policy should be directed to the Company Secretarial Department (ailegal@ckah.com).

CKA Responsible Use of GenAI Policy

- (g) The Company will review this Policy from time to time to address new developments and potential risks as GenAI tools evolve, and to ensure that it reflects any changes in applicable law, rules and regulations. The Company reserves the right to make changes to this Policy from time to time. Any amendments to this Policy will be communicated to employees by e-mail or such other means as the Company may decide from time to time.

2. Guiding Principles

The Group encourages the responsible use of GenAI tools to enhance productivity, innovation and operational efficiency. Employees using GenAI tools must observe the following principles:

- (a) comply with this Policy, all applicable law, rules and regulations, and the Group's other applicable policies;
- (b) use GenAI tools in a secure, ethical, responsible and lawful manner;
- (c) protect the Group's confidential information, intellectual property and personal data;
- (d) exercise appropriate human judgement, recognising that GenAI is intended to assist rather than replace human decision-making, and independently verify the accuracy and appropriateness of AI-generated outputs before relying on, acting upon or using them;
- (e) ensure that any AI-generated recommendations or actions (including any actions undertaken by AI assistants or AI agents) are subject to appropriate human review and approval before implementation;
- (f) ensure that the use of GenAI and AI-generated outputs is fair, objective and free from unlawful discrimination or bias, particularly where they may affect individuals;
- (g) ensure that the use of AI assistants and AI agents is subject to appropriate human oversight and controls that are proportionate to the nature and risks of their use; and
- (h) remain responsible and accountable for all work produced with the assistance of GenAI tools.

3. Employees' use of Permitted GenAI Tools

- (a) Permitted GenAI Tools may be used by employees for work-related purposes or on devices provided by the Group in line with this Policy. This includes content generation for administrative tasks, research, first drafts or designs, editing documents, summaries, brainstorming, generating ideas and other legitimate business activities. If in doubt, employees should discuss the proposed use of Permitted GenAI Tools with the relevant business unit/department head, who may approve, deny or modify the proposed use.
- (b) Employees must not use GenAI as a substitute for legal, regulatory, tax, accounting or other professional advice, or to undertake work outside their responsibilities, authority or area of expertise without appropriate oversight. Any legal, regulatory, tax, accounting or other professional research or analysis for business purposes should be undertaken by, or in consultation with, the Legal Department, Company Secretarial Department, or other relevant department, as appropriate. Employees who are not authorised to do so must not use GenAI to prepare or provide legal opinions or legal advice on behalf of the Group.

CKA Responsible Use of GenAI Policy

- (c) Permitted GenAI Tools are intended to assist, and not replace, an employee's professional judgement. Employees must review, validate and exercise independent judgment before relying on, acting upon, or using AI-generated outputs and, where appropriate, verify the accuracy of AI-generated outputs against reliable source materials. AI-generated outputs must not be relied upon as the sole basis for financial, legal, regulatory, compliance, or other material business decisions. Employees must not permit GenAI (including AI assistants and AI agents) to make decisions or take actions on behalf of the Group without appropriate human review and any required approvals. Any concerns regarding AI-generated outputs may be raised through the Group's established reporting and escalation processes.
- (d) Employees must comply with all IT Department requirements regarding the configuration and use of Permitted GenAI Tools, including any security, privacy and data governance requirements. Employees must not circumvent or disable any security or other controls implemented by the IT Department in relation to Permitted GenAI Tools. The IT Department may from time to time issue additional guidance or restrictions regarding specific Permitted GenAI Tools, access to particular GenAI tools, or emerging security risks. Employees must comply with such guidance or restrictions and remain vigilant against fake apps, phishing websites or other malicious services purporting to be legitimate GenAI tools.
- (e) To the extent that any internal work product has been generated in whole or in part by using any Permitted GenAI Tool, employees should consider whether it is appropriate, having regard to the nature, purpose and intended audience of the work product, to include a statement acknowledging the use of such Permitted GenAI Tool as a matter of good practice to maintain transparency. Employees must ensure that any AI-generated content or outcomes of AI-assisted processes are clearly identified where required to comply with applicable legal, regulatory or contractual requirements or the Group's other applicable policies.
- (f) Employees must ensure that any external communication or work product generated, in whole or in part, using a Permitted GenAI Tool must comply with applicable legal, regulatory or contractual requirements or the Group's other applicable policies.

4. Potential risks associated with the use of GenAI and mitigating measures

Employees should ensure that they have an understanding of the capabilities and potential risks associated with the use of GenAI before using any Permitted GenAI Tool for work-related purposes or on devices provided by the Group. The table below provides a non-exhaustive list of certain potential risks associated with the use of GenAI, and mitigating measures to minimise such risks that employees must follow when using Permitted GenAI Tools. Human oversight remains a key mitigating measure.

CKA Responsible Use of GenAI Policy

Potential Risks	Measures
Breach of confidentiality and legal privilege: Information provided to GenAI tools may be retained, processed or disclosed in circumstances beyond the Group’s control. Inputting confidential or legally privileged information of the Company, the Group, or the Company’s or Group’s customers or counterparties, into GenAI tools may compromise its confidentiality or legal privilege. Such information, including prompts, chat histories and AI-generated outputs, may also become subject to disclosure in legal proceedings, regulatory investigations or other legal processes. This may breach your obligation, or the obligation of the Company or the Group, to protect confidential or legally privileged information, and could expose the Company and/or the Group to significant legal, regulatory, commercial and reputational risks.	Employees must NOT input, upload or otherwise disclose any confidential or legally privileged information of the Company, the Group, or the Company’s or Group’s customers or counterparties into any GenAI tool, except where expressly permitted by the IT Department in accordance with applicable Group policies. This includes copying and pasting such information, uploading documents or files containing such information, or otherwise making such information available to GenAI tools. Employees must comply with all IT Department requirements and guidance relating to the use of Permitted GenAI Tools and the handling of data. Departments are advised to classify and encrypt documents that contain confidential information in order to add another layer of protection in case such documents are inadvertently uploaded to GenAI tools. Any technical questions in relation to encryption should be directed to the IT Department (aisupport@ckah.com). For further guidance on what constitutes confidential information and how it should be treated, please refer to the “Employee Handbook”, the “Employee Code of Conduct”, the “Policy on Handling of Confidential Information, Information Disclosure, and Securities Dealing”, and the “Information Security Policy”.

CKA Responsible Use of GenAI Policy

Potential Risks	Measures
Personal data and privacy violation: Inputting personal data (i.e. information which relates to a living individual and can be used to identify that individual) about employees, customers or other parties into GenAI tools may release such information into the public domain and create privacy risks. This could lead to breach of applicable data protection law, rules and regulations, and result in risk and liability for the Company and/or the Group.	Employees must NOT input into GenAI tools any personal data about employees, customers or other parties. Departments are advised to classify and encrypt documents that contain personal data in order to add another layer of protection in case such documents are inadvertently uploaded to GenAI tools. Any technical questions in relation to encryption should be directed to the IT Department (aisupport@ckah.com). For further guidance on what constitutes personal data and how they should be treated, please refer to the “Employee Code of Conduct”.
Infringement of intellectual property rights: GenAI tools may produce outputs that incorporate or are derivative of works protected by intellectual property rights. The Company and/or the Group could be held liable for using such outputs without the consent of the intellectual property right holders.	Employees must endeavour to produce original works created through their own skill, judgement and effort, and must treat all outputs generated by GenAI tools as a starting point rather than a finished product. Employees must not assume that AI-generated outputs are free from third-party intellectual property rights and must ensure that their use of AI-generated outputs does not infringe such rights, including by reproducing or using third-party copyrighted material or trademarks without appropriate authorisation. For further guidance on intellectual property rights, please refer to the “Employee Handbook”.

CKA Responsible Use of GenAI Policy

Potential Risks	Measures
Inaccurate, misleading or fabricated outputs: GenAI may generate inaccurate, incomplete, outdated, unreliable or fabricated information, including fictitious facts, cases, authorities, citations, references or sources, in a convincing manner. Employees may inadvertently rely on such outputs, resulting in incorrect business decisions, legal or regulatory non-compliance, financial loss, reputational damage or other risks to the Group.	Employees must treat all AI-generated outputs as a starting point rather than a finished product. Employees must always review, proofread and independently verify the factual accuracy, reliability and completeness of all AI-generated outputs before using or relying on them for business purposes. Where appropriate, employees should consult the relevant business unit or department before using or relying on such outputs.
Bias and discrimination: GenAI may generate biased, discriminatory, harmful or offensive outputs, particularly where they are used to assess or make recommendations about individuals.	Employees must NOT use any output from GenAI tools if it is biased, discriminatory, harmful or offensive, or inconsistent with the Company's purpose, culture and values.

5. Prohibited use

Employees are prohibited from using GenAI for work-related purposes or on devices provided by the Group in ways that may undermine the security or reputation of the Company or the Group, or in a manner that is inconsistent with this Policy. In particular:

- (a) Employees must not use GenAI to engage in activity that violates the privacy of others, or attempt to create or share content that could violate the privacy of others, including disclosure of personal data, or attempt to use GenAI for facial identification, or identification verification purposes, or input photographs or video/audio recordings of others taken without their consent for the processing of their biometric identifiers or biometric information.
- (b) Employees must not use GenAI to infringe on the rights of others, or attempt to use GenAI to infringe on others' legal rights, including intellectual property rights.
- (c) Employees must not use GenAI to do anything illegal. Employees must not attempt to circumvent any blocks that may be placed by the Group to dissuade illegal and/or inappropriate activity.

CKA Responsible Use of GenAI Policy

- (d) Employees must not use GenAI to engage in fraudulent, false, misleading or manipulative activity, to exploit the vulnerabilities of individuals or groups, to facilitate social scoring, or to create or share content that could mislead or deceive others, including disinformation, content enabling fraud or deceptive impersonation. Employees must not use GenAI maliciously or unethically, such as creating realistic fake content, which can be used to spread misinformation or manipulate public opinion.
- (e) Employees must not use GenAI to engage in activity that is harmful to others, or attempt to create or share content that could be used to harass, bully, abuse, threaten, or intimidate others, or otherwise cause harm to others.
- (f) Employees must not use GenAI to create or share inappropriate content or material, or content that is disturbing or offensive.

6. Copyright infringement and Policy violation

Employees must promptly report any suspected or actual copyright infringement or claim relating to the use of Permitted GenAI Tools for work-related purposes or on devices provided by the Group as well as any concerns or suspected or actual non-compliance with this Policy, to the IT Department (aisupport@ckah.com) and the Company Secretarial Department (ailegal@ckah.com).

7. Training

Training will be organised by the IT Department and/or posted at Company Intranet to help employees understand the use of Permitted GenAI Tools.

8. Non-compliance with this Policy

The Company takes compliance with this Policy very seriously. Any non-compliance with this Policy will be dealt with appropriately, taking into account the nature and circumstances of each case and the severity and impact of the non-compliance, with an emphasis on prevention of future infractions.

9. Responsibility for this Policy

This Policy has been reviewed, approved and adopted by the Board of Directors. The Audit Committee oversees and monitors the implementation and enforcement of this Policy, and may recommend revisions to the Board for approval from time to time.

Effective on: February 2024

Updated on: August 2026