# CK Asset Holdings Limited

# GenAI Use Policy

This GenAI use policy (this "**Policy**") has been developed by CK Asset Holdings Limited (the "**Company**") for the Company and its subsidiaries (collectively the "**Group**").

## 1. Introduction

1.1 Generative Artificial Intelligence ("**GenAI**") is a term that refers to artificial intelligence products that can generate new and often creative content such as text, images or music based on patterns and examples from existing data.

1.2 The purpose of this Policy is to establish guidelines for the use of GenAI tools by employees for work-related purposes or on devices provided by the Group, and to ensure that such GenAI tools are used by the employees in an ethical, responsible and lawful manner, in compliance with all applicable law, rules or regulations, and company policies. 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.

1.3 Employee access to GenAI tools for work-related purposes or on devices provided by the Group is restricted to those GenAI tools that are listed by the IT Department in the Company's intranet from time to time ("**Permitted GenAI Tools**"). 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.

1.4 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 their own independent GenAI use policy in compliance with the law, rules and regulations of the jurisdictions in which they operate.

1.5 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).

1.6 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. Employees' use of Permitted GenAI Tools

2.1 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, generating ideas and other legitimate activities. If in doubt, employees should discuss the parameters of their proposed use of Permitted GenAI Tools with the relevant business unit/department head, who may approve, deny or modify those parameters.

2.2 When employees use Permitted GenAI Tools for work-related purposes or on devices provided by the Group, they must be used in an ethical, responsible and lawful manner, in compliance with all applicable law, rules or regulations, and company policies.

2.3 The IT Department may from time to time issue special warnings regarding the use of certain specific Permitted GenAI Tools for work-related purposes or on devices provided by the Group. In particular, employees must beware of fake apps and phishing websites posing as known GenAI.

2.4 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 to include a statement acknowledging the use of such Permitted GenAI Tool as good practice to maintain transparency.

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

Employees should ensure that they have a basic 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 is a key mitigating measure to minimise such risks.

| Potential Risks | Measures |
|---|---|
| **Breach of confidentiality**: Information that is inputted into GenAI tools may enter into the public domain. Inputting confidential information of the Company, the Group, or the Company's or Group's customers or counterparties, into GenAI tools may release such information into the public domain and result in such information losing their confidentiality. This may breach your obligation, or the obligation of the Company or the Group, to keep such information confidential, and could result in significant risk and liability for the Company and/or the Group. | Employees must NOT input into GenAI tools any confidential information of the Company, the Group, or the Company's or Group's customers or counterparties. This includes copying and pasting such information to GenAI tools or uploading documents containing such information to GenAI tools. Employees must adhere to the guidelines provided by the IT Department from time to time when inputting data into Permitted GenAI tools. |

| Potential Risks | Measures |
|---|---|
| | 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).<br><br>For further guidance on what constitutes confidential information and how they 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". |
| **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.<br><br>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).<br><br>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 labour/effort, and must treat all outputs generated by GenAI Tools as a starting point and not as a finished product. Employees must also ensure that such outputs do not incorporate or display third-party trademarks. |

| Potential Risks | Measures |
|---|---|
| | For further guidance on intellectual property rights, please refer to the "Employee Handbook". |
| **Inaccuracy**: GenAI may generate inaccurate, incomplete, unreliable or outdated results in a convincing manner. | Employees must always review and proofread all generated output for factual accuracy, reliability and completeness before using such output. |
| **Bias and discrimination**: GenAI may generate biased and/or discriminatory results that might be considered harmful and/or offensive. | Employees must NOT use any output from GenAI Tools if it is biased and/or discriminatory, or can be considered harmful and/or offensive, or if it does not align with the Company's purpose, culture and values. |

## 4. 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:

4.1 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.

4.2 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.

4.3 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.

4.4 Employees must not use GenAI to engage in activity that is fraudulent, false, or misleading, or attempt to create or share content that could mislead or deceive others, such as creation of 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.

4.5 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.

4.6 Employees must not use GenAI to create or share inappropriate content or material, or content that is disturbing or offensive.

## 5. 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 of this Policy, to the IT Department (aisupport@ckah.com) and the Company Secretarial Department (ailegal@ckah.com).

## 6. Training

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

## 7. 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.

Effective on: February 2024