



China Hongqiao Group Limited
中国宏桥集团有限公司
(根据开曼群岛法例成立的有限公司)
(「本公司」)
(股份代号: 1378)

负责任人工智能政策

(经本公司可持续发展委员会于 2026 年 10 月 9 日采纳)

一、核心理念与目标

中国宏桥集团有限公司（以下简称“中国宏桥”或“本集团”）致力于以安全、合规、透明、伦理且负责任的方式开发、部署或使用人工智能（AI）技术。本政策旨在建立全面的 AI 治理框架，规范 AI 系统的开发与应用，在支持本集团创新发展和运营效率提升的同时，以合理方式识别和缓解相关潜在风险，维护利益相关方的合法权益，并促进企业可持续发展。

二、编制依据

本政策依据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《生成式人工智能服务管理暂行办法》《人工智能生成合成内容标识办法》，并参考经合组织人工智能原则（OECD AI Principles）、联合国人工智能伦理建议（UN Recommendation on the Ethics of Artificial Intelligence）、欧盟《人工智能法案》（EU AI Act）等国际标准及相关适用的法律法规制定。

三、适用范围

本政策适用于中国宏桥集团及其下属分、子公司的全体员工（含董事会成员、高级管理人员在内的全职员工、兼职员工、实习生及劳务派遣人员），覆盖研发、采购、生产、运营、销售及服务等全价值链环节的各类应用场景和人工智能系统的全生命周期。同时，本集团亦倡导并推动价值链合作伙伴（包括供应商、承包商、客户等）共同遵循本政策理念，协同推动负责任人工智能的开发与应用。

四、承诺与行动

本集团各单位在开发、部署或使用人工智能系统时，遵循并落实以下管理原则：

1. 严格保护数据隐私

在 AI 系统的开发、训练、部署及使用过程中，严格保护数据隐私，确保个人信息及相关数据的收集与处理遵守运营所在地数据保护相关法律法规。未经批准，不得将本集

团商业秘密及其他敏感信息输入外部 AI 工具；使用第三方模型时，须严格约定数据用途、留存和删除要求，未经授权不得将本集团数据用于模型训练或其他用途。本集团建立数据分类分级管理机制，根据数据敏感程度，严格执行匿名化或去标识化处理，并采取脱敏、访问控制、隐私计算等适当措施，对 AI 数据的全生命周期实施安全管控。

2. 强化网络安全保障

本集团将 AI 系统、模型、工具及相关基础设施全面纳入网络与信息安全防护体系，通过核心数据加密、最小权限访问等措施，防范未经授权访问、数据泄露、数据篡改、模型窃取和恶意攻击等安全威胁。本集团定期开展安全评估与应急演练，建立输入输出安全检查、内容过滤和异常行为检测机制以及应急响应机制，形成多层次安全防护体系。对于采购或合作使用的第三方 AI 平台、模型及服务，本集团审慎评估其资质与合规能力，避免因 AI 应用引发的网络与信息安全事故对用户权益、企业运营及公共利益造成损害。

3. 主动识别与避免算法偏见

本集团高度关注 AI 在数据采样、模型设计与输出结果中可能存在的偏见、歧视与误导风险，在 AI 模型开发环节，使用多样化数据集以提升结果公正性，并对已部署的 AI 模型定期开展公平性评估或偏见测试。同时，结合 AI 应用场景，采取人工复核和纠偏等有效措施识别、评估和缓解潜在偏见，确保 AI 决策及输出符合公平性要求。

4. 坚持人类在关键决策中的核心地位

针对重大生产经营决策、安全生产及对利益相关方产生重要影响的 AI 应用场景中，本集团坚定落实重大决策责任仍由人承担的管理机制。涉及自动控制的 AI 应用，应经过验证和授权，明确运行范围，保留必要的安全联锁、人工接管和异常退出措施。AI 不得绕过既有业务审批和安全保护机制，在缺少人工监督、人工复核及否决机制的前提下做出不可撤销或高风险的重大决策。

5. 提升系统透明性与结果可解释性

本集团承诺在技术可行范围内提升 AI 系统的透明度，并按需（如按适用法律法规和发布平台需求）披露 AI 的用途、能力、局限性、数据来源及风险，采取适当的标识；针对 AI 生成结论，尽可能提供基础逻辑说明，便于利益相关方理解 AI 输出的局限性；对外发布的重要内容须经人工审核，并保留必要的来源和审核记录，确保内容可追溯、可核查。

6. 确立清晰的责任追溯与异议申诉机制

本集团建立清晰的 AI 应用责任分配机制，对每项 AI 应用明确业务负责人与技术负责人，对 AI 模型或工具产生的结果明确责任归属，确保业务决策责任可追溯。本集团亦制定错误或危害事件的调查、责任承担机制与补救流程。本集团已出台《利益相关方投诉处理制度》《举报政策》等制度文件，搭建覆盖员工、外部利益相关方的投诉处置

流程，规范投诉受理、核查、整改、反馈全流程。利益相关方如对 AI 决策存在异议、认为自身权益受 AI 应用影响，可依托现有制度渠道提交诉求；由本集团对应管理部门开展内部核查、责任判定与整改跟进，留存处置档案，实现 AI 相关问题闭环管理。

7. 严明 AI 技术应用边界与功能限制

本集团建立 AI 系统授权管理与能力边界控制机制，防范越权滥用及非预期应用。AI 应用上线前，须完成数据安全、算法合规及效果验证，由业务单位确认使用范围并验收通过后方可上线；涉及生产安全、生物识别或自动执行等高风险场景的，需履行专项评估及授权程序。当模型、知识库或应用范围发生重大变更时，须重新开展评估验证。针对具备核心系统调用能力的 AI 智能体，严格限制其仅在授权范围内执行任务，关键操作设置人工审批与留痕机制。

8. 持续降低 AI 算力的生态足迹

在使用自有或第三方 AI 数据中心及模型时，本集团优先选择及鼓励使用节能、高效的设施与技术方案，鼓励使用可再生能源，逐步优化 AI 系统的生态足迹，降低能源消耗、水资源使用、碳强度以及对环境的影响。

本集团视内部管理需求，定期统计 AI 算力节能降耗、数字化减排、资源节约等相关数据，测算 AI 应用对可持续管理目标的贡献，在具备条件的情境下，将相关统计成果纳入年度 ESG / 可持续发展报告对外披露。

9. 严禁部署违法及非正当用途系统

本集团承诺不开发、部署或使用以下 AI 系统或应用：

- (1) 具有操纵性行为，采用超越个人意识的操纵性或欺骗性技术，实质性扭曲个人行为并可能造成危害的 AI 系统；
- (2) 利用特定群体（年龄、残疾、社会经济处境等）脆弱性造成伤害的 AI 系统；
- (3) 基于社会行为或个人特质进行社会评分，导致不公正待遇的 AI 系统；
- (4) 未经合法授权开展生物特征识别、面部识别监控或其他生物识别监视活动的 AI 系统；
- (5) 违反法律法规、监管要求、伦理规范及集团制度的其他 AI 系统和应用。

此外，涉及生产安全、人员权益等高风险场景的 AI 应用，须经专项评估和授权，并接受持续监督。

10. 负责任 AI 文化建设与持续改进

本集团面向内部员工按需开展 AI 伦理、安全合规培训，将 AI 合规及安全使用纳入企业安全文化建设体系，持续提升员工对 AI 风险识别与合规使用的认知水平与实操能力。

同时，本集团按 AI 应用场景开展运行监测、抽样检查和定期评测，重点检查错误输出、误报漏报及异常调用，并及时优化整改，实现管理闭环。一经发现风险隐患，视情况采取调整知识库、限制功能、切换模型或停用等处置措施，并记录处理结果。对供应商模型发生的重大变更，须重新开展验证评估，确保 AI 系统持续满足性能、安全与合规要求。

五、附则

1. 持续改进

本集团将视需根据法规变化、行业标准更新及利益相关方反馈，对本政策进行适时修订，并通过官网、ESG 报告/可持续发展报告等渠道公开更新内容，以确保政策的持续适应性与有效性。

2. 审批机构

本政策经本集团董事会下辖可持续发展委员会审议通过，自发布之日起实施。

3. 解释

本政策由中国宏桥负责解释。文件以中文及英文编制，如有内容差异，应以中文文本为准。