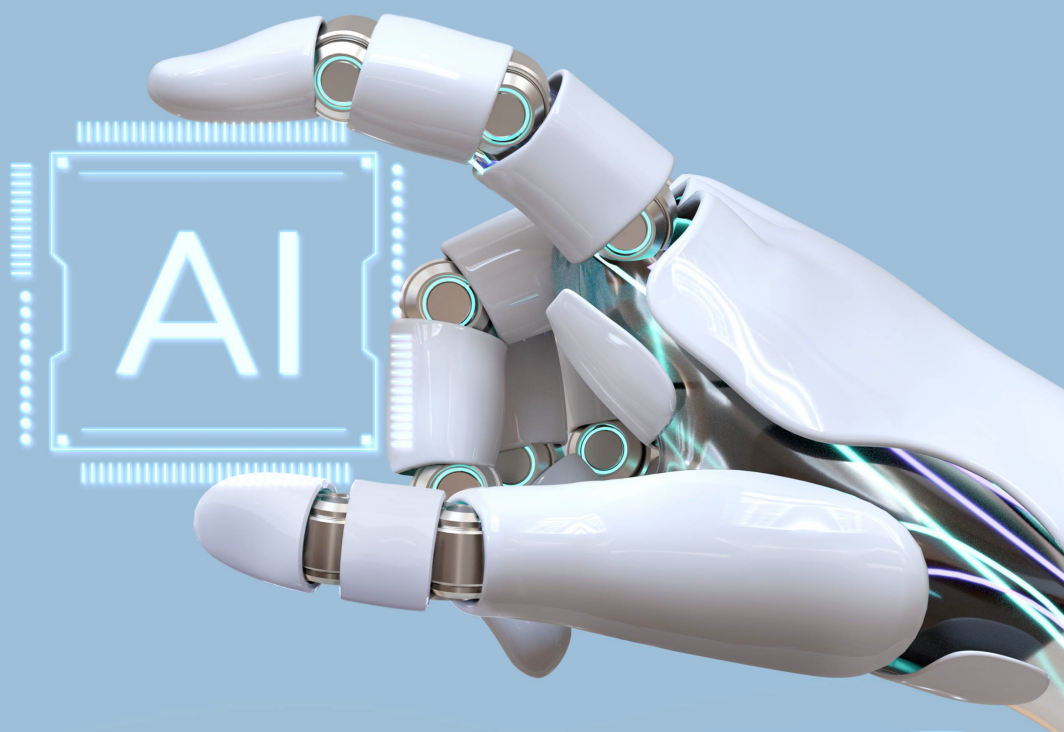


政府部门 人工智能应用指南

人工智能推动政务服务转型



数字政策办公室

二零二六年七月

行动呼吁

人工智能技术的迅速发展为政务服务带来前所未有的机遇，可以优化传统流程、提升效率、改善决策，并提供更优质的公共服务。采用人工智能技术可以帮助组织在瞬息万变的环境中保持竞争力、迅速反应和创新能力。各决策局／部门（局／部门）应将人工智能视为推动业务转型、提升业务效率和改善服务质素的策略性技术。通过从上而下的领导层推动及以业务主导的「人工智能+」策略，积极迎接人工智能及改革部门各方面的运作流程和服务方式，局／部门可以提升效率、精简工作流程、优化资源配置，并促进政府使用更灵活、更具前瞻性的治理方法，最终令市民和整个社会受益。

我们呼吁各局／部门善用人工智能，共同建设智慧政府。

关键原则

在展开这个变革旅程时，我们建议各局／部门遵循以下关键原则：

采用更多**合适**的人工智能解决方案，以提升公共服务的**成本效益**



推动更多**人工智能+业务流程改革**以优化工序



采取**业务主导和成果为导向**的方针，实现明确的业务目标



确保**安全及合乎道德**地采用人工智能，以管理和降低风险



采用策略

1

采用现成的人工智能解决方案

我们鼓励各局／部门善用市场上现成的人工智能解决方案，加快人工智能应用进程以提升运作及公共服务效率，同时省却投入大量开发资源。此外，市场上的解决方案通常提供完善的支援和更新服务，确保长期可持续性。

例如：

- 「香港生成式人工智能研发中心」(HKGAI)的「港文通」、「港话通」及「港会通」
- 数字人、会议工具、人工智能文件处理、光学字符识别(OCR)、简报生成器等

2

开发专属的人工智能应用以满足特定需求

对于具有特定业务需求和安全要求的局／部门，可能需要使用结合特定领域知识的定制人工智能方案。局／部门可以采用以专门领域知识和内部数据训练的垂直人工智能模型，并开发专属的人工智能应用程序，以满足其特定的业务需求。专属的人工智能应用程序让各局／部门能够根据其独特需求定制人工智能解决方案，推动创新和卓越营运。

例如：

- 局／部门的知识管理系统和内部聊天机械人
- 用于进行异常检测的影像分析应用
- 用于进行检查和危险行动的人工智能机械人

基础设施配套：

- 政务云平台

安全且负责任地采用人工智能

为了实现效益并避免不良后果，建议各局／部门遵循相关指引中规定的建议和推荐做法，在促进人工智能创新应用的同时，采取平衡方针以保障公众利益和降低潜在风险：

《人工智能道德框架》

《香港生成式人工智能技术及应用指引》



采用人工智能的周期

- 1 **以业务主导识别采用人工智能的机遇：**从合适业务范畴领导分析现有工作流程和服务，识别人工智能可以创造价值并配合策略目标的范畴。
- 2 **搜寻合适的人工智能解决方案：**研究并评估具成本效益、可信赖且有利的人工智能技术，以满足特定的业务需求。
- 3 **选择解决方案供货商：**选择具有丰富专业知识、致力于推行负责任的人工智能实践，并能提供完善支援服务的供应商，以确保方案成功实施。
- 4 **测试、评估和验证：**进行全面测试和试行计划，以评估表现、收集意见，并根据预设的成功准则以验证结果。
- 5 **部署、营运和持续改善：**分阶段部署人工智能解决方案以管理风险，培训员工，并制定维护计划以进行持续监察和改进。

局／部门使用人工智能的指引



确保人工智能系统的服务符合相关法例、法规、组织政策及道德安全规范，同时遵循私隐保障和资讯保安政策、安全标准和操作程序等要求。

监督、维护及审计人工智能系统，包括更新、优化、安全性修补等，确保其持续符合服务要求和组织目标。

制定清晰的紧急应变程序，以便迅速处理异常、安全漏洞或道德问题。

指派受过训练的员工作为负责人，监督人工智能系统的生命周期。



建議員工審查及核實生成式人工智能工具所生成的资讯（例如新聞稿、報告），以確保其準確性。

提醒员工生成式人工智能工具所生成的输出可能存在人工智能幻觉及包含偏见、不准确或歧视性的资讯，因此他们必须审查并在必要时进行修正。



向员工提供安全及适当地使用人工智能的实用建议、例子及培训。

确保员工了解人工智能工具的能力、限制及相关风险。虽然人工智能可以提升工作效率和质量，但它仍然是一种辅助工具，不能取代员工的责任。

用户使用生成式人工智能的「应做」和「不应做」事项

应做



- ☐ **积极在工作中应用人工智能**
鼓励各层级人员正面认识不同人工智能工具的功能与局限（包括学习高效的人工智能提示语撰写技巧），在日常工作中积极探索利用合适人工智能工具提升工作效能和革新工作流程。
- ☐ **验证人工智能生成内容的准确性**
在采用人工智能生成的内容前，必须与官方及可信来源进行核实，以确保资料准确无误。
- ☐ **保护敏感及机密资料**
切勿将机密或个人资料输入外部或公共人工智能平台。在处理敏感数据时，应先移除或遮盖可识别的细节，才可使用相关人工智能工具。
- ☐ **了解使用条款及私隐政策**
阅读并理解人工智能工具的使用条款及私隐政策，以便更详尽了解人工智能工具服务提供者的数据处理方式及相应的用户责任。
- ☐ **主动管理数据私隐**
定期检视并删除人工智能工具中的对话记录或储存的数据，以减低私隐风险及数据泄露的可能性。
- ☐ **遵守政府规定及指引**
严格遵守个人资料（私隐）条例、资讯保安和人工智能道德相关的规定及指引，以确保合法及合乎道德地使用人工智能工具。



不应做



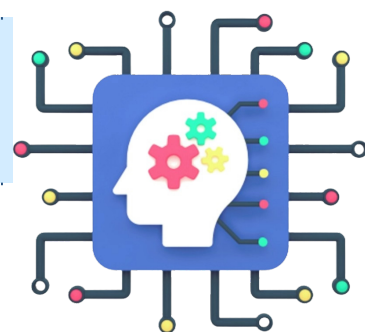
- ☐ **不应指示人工智能生成侵犯版权的内容**
避免使用人工智能复制或创作可能侵犯版权材料或知识产权的内容。
- ☐ **切勿将人工智能用于不道德或非法的用途**
不要使用人工智能生成具歧视性、冒犯性或违反政府行为守则及法律的内容。
- ☐ **切勿完全依赖人工智能作出重要决策**
在作出重要决定时，尤其是关于政策制定、法律事务或关键操作方面，切勿完全依赖人工智能的输出而不经人工审查。

智能体的「应做」和「不应做」事项

应做



- ☐ **定义资料分类级别并指派予智能体**
按资料敏感度进行分类（非保密、限阅、机密等），并在使用任何智能体前，预先定义智能体获准存取的级别。
- ☐ **定期检查记录以监察智能体行为**
保留智能体在执行每项任务时的纪录，包括用户名称、输入内容、输出结果及操作时间，根据系统记录定期（建议每季一次）监察智能体的表现，包括准确度、公平性指针及模型漂移迹象等。
- ☐ **收集智能体的数据传输详情**
智能体供货商须在合约列明资料所在地、跨境传输安排、智能体可存取的系统及模型训练数据来源。
- ☐ **为持份者安排定期培训**
为不同岗位人员（决策层、管理层、操作人员与技术人员）提供人工智能专业能力培训，针对智能体功能、自主界限、潜在风险及最新政策等每年进行培训。
- ☐ **实施最低权限原则**
仅赋予智能体其任务所需、特定的“技能”（工具/功能），优先赋予只读权限而非高权限，并将需要高权限操作的技能（不可逆转的操作、外部通讯、付款）置于人工审查与批准之后。
- ☐ **使用官方渠道提供的智能体或插件**
从官方渠道下载并安装最新稳定版本的智能体软件或插件，并定期检查及修补漏洞，同时关注官方安全公告，以减低资料外泄的机会。



不应做



- ☐ **切勿在智能体指令或配置写入敏感资料**
切勿在任何智能体指令或连接的工具配置中写入内部系统标识码、API 凭证或个人标识资讯。
- ☐ **未经人工审核不得向公众发布内容**
禁止智能体在未经明确来源标示与人工审核机制的情况下发布公开内容。
- ☐ **避免对智能体授权过度权限**
切勿授权开放式的高风险权限（例如：执行任意程序代码、不限制资料库存取）予智能体，同时避免单一智能体结合多种敏感技能以防触发高风险行为（例如：读取机密资料后对外发送）。
- ☐ **切勿将未经加密的智能体连接到互联网**
除非有明确需要，且已采取适当的安全控制，否则不得将智能体直接连接到互联网。在此情况下，存取应透过加密通道、限制来源 IP、强密码、数位凭证或硬体安全密钥加以保护。

人工智能提示语撰写技巧



为何优质提示语很重要？

清晰且有效的提示语能协助生成式人工智能工具提供准确、适切和有用的回应。这就像向同事提供清晰的指示一样！请参考以下撰写有效提示的技巧。

1. 具体明确	清楚说明你的需求。 ✗ 「告诉我关于网络安全。」 ✓ 「列出公务员远程工作首5个网络安全最佳实务指引。」
2. 提供上文下理	包含相关细节（例如：受众、范围、背景、任务）。 ✗ 「草拟一份私隐政策。」 ✓ 「为一个收集市民健康数据的手机应用程序草拟一份一页的私隐政策。」
3. 指定角色	指示人工智能以专家身份回应。 例子：「以法律顾问的身份，总结政府部门与非政府组织共享数据时的数据私隐影响。」 注意：角色指定不适用于推理模型，因为这可能会影响其推理逻辑。
4. 加入限制条件	定义决策规则。 例子：「如果从指引中找不到相关资讯，绝对不可凭空捏造指导原则。若不确定，请勿捏造答案。」
5. 定义格式	指明字数和格式要求。 例子：「以四栏表格（国家／经济体系、方法、优点、缺点）比较三个国际人工智能道德框架，包括内地、美国和英国。」
6. 持续尝试	若输出的内容未如理想，请尝试调校提示语，或提供更多上文下理，要求人工智能重新生成有关内容，并明确指出需要改进的地方。 例子：「添加简短结论并采用正式语气。限于500字。」

人工智能提示语撰写技巧

使用示例

角色

格式

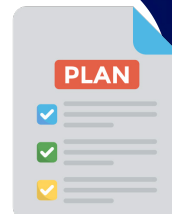
上文下理

条件

1

草拟全城回收计划的行动方案

以高级环境保护主任的身份，撰写分步骤推行的行动方案（以要点形式列出），篇幅为一页，供政府人员实施全城回收计划。内容应包括社区参与、资源分配和进度监察等阶段。方案应简明扼要及切实可行。



2

草拟处理怀疑钓鱼电邮的程序

以政府资讯科技保安主任的身份，以编号列表方式拟定一项分步骤程序，篇幅为一页，供部门员工安全处理及举报怀疑钓鱼电邮。内容应包括识别方法、即时行动、举报渠道和跟进措施。程序应简明扼要，适合具备基本资讯科技知识的员工遵循。



便利措施

人工智能的应用和解决方案



智慧政府创新实验室
Smart Government Innovation LAB



「香港生成式人工智能
研发中心」(HKGAI)

- [人工智能方案目录](#)
- 「AI+ 政务」计划

- 本地开发的 HKGAI 模型
- 一系列的工具有「港文通」、「港话通」、「港会通」等



优质资讯科技专业
服务常备承办协议
(SOA-QPS)

构建服务

- 用于采购内部人工智能应用开发的资讯科技服务合约

基础设施



政务云平台

应用部署

- 政务云平台



授权数据交换闸

数据交换

- 授权数据交换闸(CDEG)

人工智能算力资源



政务云平台

- 数码港人工智能超算中心
- 政府云端设施服务 - 多元化信息科技基础设施服务

数据



開放數據平台
DATA.GOV.HK

- [开放数据平台](#)
- 部门数据目录

安全且负责任地采用人工智能



指引

- [《人工智能道德框架》](#)
- [《香港生成式人工智能技术及应用指引》](#)