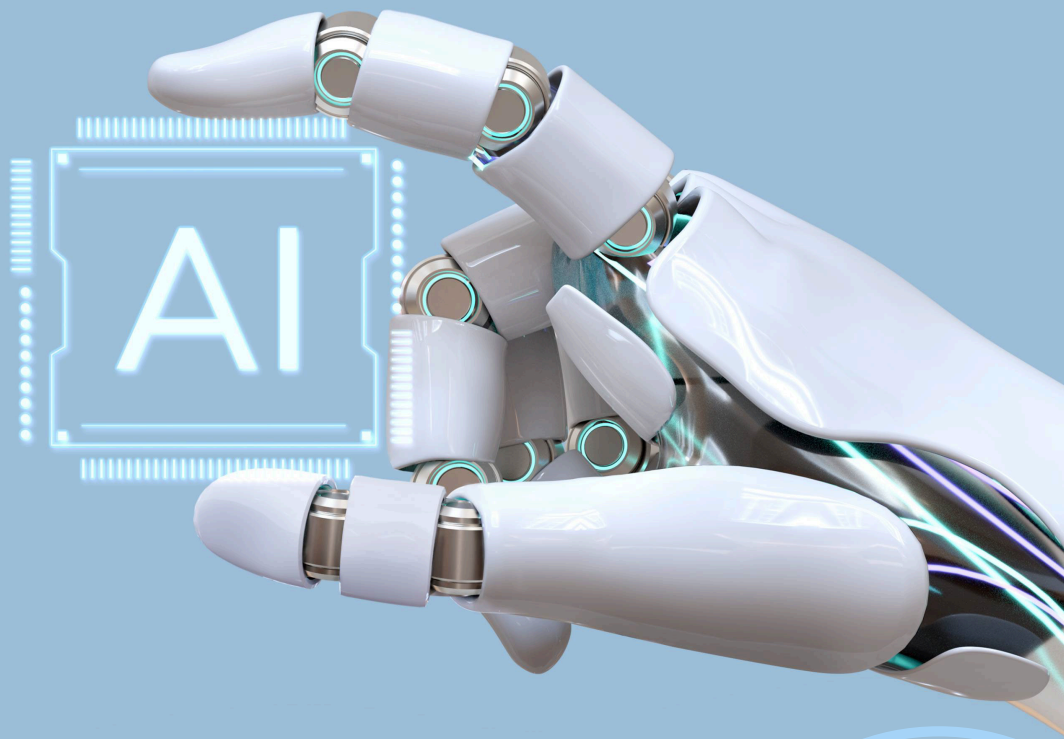


Artificial Intelligence Adoption Guide for Government Bureaux and Departments

**Civil Service Transformation
through AI**



Digital Policy Office

July 2026

Call for Action

The rapid advancement of artificial intelligence (AI) technologies presents unprecedented opportunities for Civil Service to transform traditional processes, enhance efficiency, improve decision-making, and deliver better public services. Adopting AI can help organisations to stay competitive, responsive, and innovative in a rapidly changing landscape. Bureaux and departments (B/Ds) should view AI as a strategic technology for enabling business transformation, enhancing business efficiency and improving quality of services. Through top-down leadership drive and business-led “AI+” approach to actively embrace AI and undertake business transformation in different work processes and public services, B/Ds can enhance efficiency, streamline workflows, optimise resource allocation, and foster a more agile, forward-thinking approach to governance, ultimately benefiting citizens and society as a whole.

We call for all B/Ds’ action in leveraging AI to jointly develop a Smart Government.

Key Principles

As we embark on this transformative journey, we recommend B/Ds should follow these key principles:

Adopt more **suitable** AI solutions to enhance **cost-effectiveness** of public services



Drive more **AI+business process transformation** to optimise workflows



Be **business-led and result-oriented** in meeting clear business objectives



Ensure **safe and ethical adoption of AI** to manage and reduce risks



Adoption Strategy

1

Adopt Readily Available AI Solutions

B/Ds are encouraged to leverage readily available AI solutions from the market to accelerate their AI journey in process and service enhancement without requiring substantial development efforts. Additionally, market solutions often come with robust support and updates, ensuring long-term sustainability.

Examples:

- Hong Kong Generative AI Research and Development Center (HKGAI)'s HKPilot, HKChat and HKMeeting
- Digital person, meeting tools, AI document processing, Optical Character Recognition (OCR), presentation generator, etc.

2

Develop Bespoke AI Applications to meet specific needs

For B/Ds with specific business needs and security requirements, customised use of AI with domain specific knowledge may be required. B/Ds can adopt vertical AI models, trained with domain specific knowledge and internal data, and develop bespoke AI applications to meet their specific business needs. Bespoke AI applications allow B/Ds to tailor AI solutions to their unique requirements, driving innovation and operational excellence.

Examples:

- B/D's knowledge management system and internal chatbot
- Image analytics applications for abnormality detection
- Robotics with AI for inspection and dangerous operations

Supporting Infrastructure:

- Government Cloud Platform

Safe and Responsible AI Adoption

To realise the benefits and avoid adverse outcomes, B/Ds are advised to adopt AI with a balanced approach for safeguarding public interest and mitigating potential risks while facilitating innovation, by following the recommendations and suggested practices as stipulated in the related guidelines:

Ethical Artificial Intelligence Framework

Hong Kong Generative Artificial Intelligence Technical and Application Guideline



AI Adoption Lifecycle

- 1 Identifying Business-led Opportunities for AI Adoption:** Identify business area to lead analysis of existing workflows and services to pinpoint areas where AI can drive value and align with strategic goals.
- 2 Sourcing Appropriate AI Solutions:** Research and evaluate cost-effective, trustworthy and beneficial AI technologies that meet specific business needs.
- 3 Choosing a Solution Provider:** Select a provider with proven expertise, strong commitment to responsible AI practices, and robust support services to ensure successful implementation.
- 4 Testing, Evaluation, and Validation:** Conduct thorough testing, pilot runs to assess performance, gather feedback, and validate results against predefined success criteria.
- 5 Deployment, Operations, and Continuous Improvement:** Deploy AI solutions in phases to manage risk, train staff, and establish a maintenance plan for continuous monitoring and improvements.

Guidelines for Using AI by B/Ds



Ensure AI system services comply with relevant laws, regulations, organisational policies, and ethical standards, while adhering to privacy protection, information security, safety standards, and operational procedures.

Monitor, maintain and audit the AI system, including updates, optimisation, security patch, etc., to ensure continuous alignment with service requirements and organisational goals.

Establish clear emergency response procedures to promptly address anomalies, security breaches, or ethical issues.

Designate trained staff as the responsible personnel to oversee the AI system's life cycle.



Advise staff to review and conduct fact-checking for information generated by generative AI tools (e.g. press releases, reports) to ensure its accuracy.

Remind staff that the generated output of generative AI tools may have AI hallucination and contain information that are biased, inaccurate or discriminatory, for which they must review and correct if deemed necessary.



Provide staff with practical advice, examples and training on how to use AI safely and appropriately.

Ensure staff understand the capabilities, limitations and risks associated with AI tools. While AI can enhance work efficiency and quality, it remains a supportive tool and does not assume the responsibilities of staff.

DOs and DON'Ts for Using Generative AI by End Users

DOs



- ☐ **Proactively Adopt AI in Work Place**
Encourage staff at all levels to positively appreciate the capability and limitation of different AI tools (including to learn effective AI prompt writing tips), and actively explore adoption of appropriate AI tools in work place to improve work efficiency and innovate work processes.
- ☐ **Verify Accuracy of AI-Generated Content**
Always cross-check AI-generated content against official and trusted sources to ensure factual correctness before adoption.
- ☐ **Protect Sensitive and Classified Information**
Don't input classified or personal data into external or public AI platforms. When working with sensitive data, remove or mask identifiable details before using AI tools.
- ☐ **Understand Terms of Use and Privacy Policies**
Read and understand the terms of use and privacy policies of AI tools to better understand the data handling practices of the service providers of AI tools and corresponding user obligations.
- ☐ **Manage Data Privacy Proactively**
Regularly review and delete chat histories or stored data in the AI tools to minimise privacy risks and data exposure.
- ☐ **Comply with Government Regulations and Guidelines**
Adhere strictly to Personal Data (Privacy) Ordinance, regulations and guidelines on information security and AI ethics to ensure legal and ethical use of AI tools.



DON'Ts



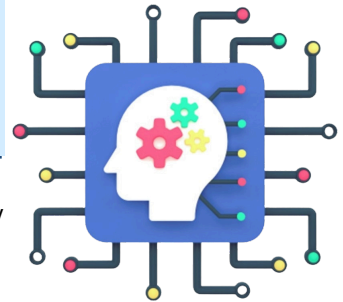
- ☐ **Don't Instruct AI to Generate Copyright-Infringing Content**
Avoid using AI to reproduce or create content that may infringe on copyrighted materials or intellectual property rights.
- ☐ **Don't Use AI for Unethical or Illegal Purposes**
Do not use AI to create content that is discriminatory, offensive, or violates government codes of conduct and laws.
- ☐ **Don't Rely Solely on AI for Critical Decisions**
Never depend exclusively on AI outputs without human review when making important decisions, especially for policy development, legal matters, or critical operations.

DOs and DON'Ts for AI Agents

DOs



- ☐ **Define Data Classification Level and Assign to AI Agents**
Classify data sensitivity into categories (Unclassified / RESTRICTED / CONFIDENTIAL, etc.) and map each tier to permitted AI agents' access scopes before any use.
- ☐ **Conduct Log Review to Monitor the Agent Behaviour**
Retain full execution logs of AI agents (user identity, input, output, timestamp) and conduct periodic reviews (recommended quarterly) of agent behaviour accuracy, fairness metrics, and model drift indicators based on logged data.
- ☐ **Collect Data Transmission Details of AI Agents**
Require the vendors of AI agents to disclose data residency, cross-boundary transfer, agent-accessible system integrations, and model training data sources in the contract.
- ☐ **Arrange Regular Training to All Stakeholders**
Implement role-based AI competency training (decision-makers / managers / operators / technical staff) with annual refreshers on agent capabilities, autonomy boundaries, risks, and policy updates.
- ☐ **Apply a Least-Privilege Principle**
Grant an agent only the specific, narrowly-scoped "skills" (tools/functions) needed for its task, favour read-only over high-impact ones, and gate high-impact skills (irreversible actions, external communication, payments) behind human approval.
- ☐ **Use Agents or Plugins from Official Sources**
Download and install the latest stable version of the agent software or plugin from official sources, conduct regular vulnerability checks and apply security patches, and closely monitor official security alerts to reduce the risk of data leakage.



DON'Ts



- ☐ **DON'T Include Sensitive Information in AI Agent Instructions / Configurations**
Do not include internal system identifiers, API credentials, or personally identifiable information (PII) in any AI agent instructions or connected tool configurations.
- ☐ **DON'T Publish Public-facing Content Without Approval**
Do not allow AI agents to publish public-facing content without explicit source attribution and human review mechanism.
- ☐ **DON'T Over-provision Skills to AI Agents**
Do not grant open-ended high-risk skills (e.g. arbitrary code execution, unrestricted database access), and don't let a single agent combine skills that together enable sensitive actions (e.g. reading confidential data plus sending it externally).
- ☐ **DON'T Connect Unencrypted Agents to the Internet**
Never connect agents directly to the internet except explicitly required and with proper security control. In such cases, access shall be protected by encrypted channels, restricted source IPs, strong passwords, digital certificates, or hardware security keys.

AI Prompt Writing Tips

Why Good Prompts Matter?

Clear and effective prompts help generative AI tools deliver accurate, relevant, and useful responses. Think of it like giving clear instructions to a colleague! Consider the following tips for crafting effective prompts.



1. Be Specific	Clearly state what you need. ✗ “Tell me about cybersecurity.” ✓ “List the top 5 cybersecurity best practices for remote work by civil servants.”
2. Provide Context	Include relevant details (e.g. audience, scope, background, tasks). ✗ “Draft a privacy policy.” ✓ “Draft a 1-page privacy policy for a citizen-facing mobile app collecting citizen health data.”
3. Assign a Role	Direct the AI to act as an expert. <i>Example:</i> “As a legal advisor, summarise the data privacy implications for a government department sharing data with NGOs.” Note: Role assignment is not applicable for reasoning models as it may affect its reasoning logic.
4. Add Stopping Conditions	Define decision rules. <i>Example:</i> “Never hallucinate the guiding principles if the relevant information cannot be found in the Guideline. Do not fabricate an answer if you are uncertain.”
5. Define Format	Specify word count and format. <i>Example:</i> “Provide a comparison of three international AI ethics frameworks, including the Mainland, the US and the UK, in a 4-column table (Country/Economy, Approach, Pros, Cons).”
6. Keep Trying	If the output is not satisfactory, try to refine your prompts or provide more context to ask AI to re-generate its output, specifying clearly the areas to improve. <i>Example:</i> “Add a brief conclusion and adopt a formal tone. Limit to 500 words.”

AI Prompt Writing Tips

Usage Examples

Role

Format

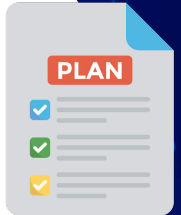
Context

Condition

1

Draft an action plan for implementing a city-wide recycling initiative

As a senior environmental protection officer, write a one-page step-by-step action plan (in bullet points) for government staff to implement a city-wide recycling initiative. Include stages such as community engagement, resource allocation, and monitoring progress. The plan should be concise and practical.



2

Draft a procedure for handling suspected phishing email

As a government IT security officer, create a one-page step-by-step procedure (numbered list) for department staff to securely handle and report a suspected phishing email. Include instructions on identification, immediate actions, reporting channels, and follow-up measures. The procedure should be concise and suitable for employees with basic IT knowledge to follow.



Facilitation Measures

AI Applications and Solutions



智慧政府創新實驗室
Smart Government Innovation LAB

- [AI Solution Catalogue](#)
- "AI+ Civil Services" Initiative



Hong Kong Generative AI
Research and Development
Center (HKGAI)

- Locally-developed HKGAI large language model
- A range of tools, e.g. HKPilot, HKChat, HKMeeting, etc.

Implementation Services



Standing Offer Agreement
for Quality Professional
Services (SOA-QPS)

- IT service term contract for procurement of service for in-house AI application development

Infrastructures



Government
Cloud Platform

Application Hosting

- Government Cloud Platform



Consented Data
Exchange Gateway

Data Exchange

- Consented Data Exchange Gateway (CDEG)

AI Computing Resources



Government
Cloud Platform

- Cyberport's AI Supercomputing Centre
- Government Cloud Infrastructure Services - Diversified Cloud Infrastructure

Data



開放數據平台
DATA.GOV.HK

- [Open Data Portal](#)
- Departmental Data Catalogue

Guidelines for Safe and Responsible Use of AI



Guidelines

- [Ethical Artificial Intelligence Framework](#)
- [Hong Kong Generative Artificial Intelligence Technical and Application Guideline](#)