Generative AI Tool Usage Policy

Reference:	GMICT P 0123	Publication:	16 June 2025
Version:	2.0	Effective:	16 June 2025

Purpose

Whilst it is understood that generative AI tools can present innovative opportunities in public services, their rapid development poses risks and challenges, that merit careful assessment and evaluation in their applicability within Public Administration. This is especially so, if the tools involve the input of Government data for purposes of machine learning or as an aid for decision making, in the conduct of services by the Public Administration. Careful considerations to ensure their trustworthy and responsible application is especially so if the tools, for justifiable reasons, are not procured through the Agent.

Scope

This Policy covers the use of generative AI tools involving **input of Government data** for machine learning and/or as support for any form of decision-making purposes **within the Public Administration**,

(i) provided through the Agent, as referred to within the *GMICT P 0121 Centralised Digital Enabling Services* Policy. The **tools provided through the Agent** are:

a) ***Microsoft Copilot***;

b) ***OpenAI services*** provided through the Agent's Cloud platform;

(ii) alternative to the tools as identified in (i) – hereby referred to as **'alternative Generative AI tools'** - in case that the ones referred to in (i) are, for justifiable reasons, not appropriate to the needs of the Public Administration organisation.

This Policy applies to:

(i) all Public Administration employees and to contractors/suppliers having access to solutions that handle Government data.

(ii) Use of generative AI tools on trusted and/or untrusted devices

This Policy shall be read in conjunction with the relevant Appendices, which outline the specific Terms of Use applicable to individual generative AI tools provided through the Agent. These Appendices form an integral part of the Policy and provide detailed guidance tailored to the specific functionalities, risks, and compliance requirements of such tools.

Definitions

Underlined terms are defined in the **Vocabulary** (GMICT X 0003).

Responsible applicability

Rationale

Effectiveness and trustworthiness of public service delivered can only be ensured if the generative AI tool is used in a responsible manner whereby the prevention of harm is a priority.

1. The intentions, consequences and risks of the application of **any** Generative AI tool is to be assessed prior and following the deployment of the technology within a Public Administration organisation.

   The use of such tools should be allowed to activities where the related risks assessed can be managed effectively.

2. The provider and technology selection requirements for any Generative AI tool shall need to address **information security**, **privacy**, **copyright**, **traceability** and **transparency / explainability** challenges.

   - **Information Security** in terms of ensuring comprehensive protection against information security threats and vulnerabilities, in line with the *GMICT P 0016 Information Security Policy*.
   - **Privacy** in terms of end user protection in line with the *General Data Protection Regulation*, the *Data Protection Act* and any other related official communications and directives issued by Government.
   - **Copyright** in terms of giving due attention on training of the AI model and related outputs, in line with relevant Copyright legislation.
   - **Traceability** in terms of the capability to track the predictions and process of the AI model.
   - **Transparency and Explainability** in terms of the capability to explain how the AI model works and the methodology it uses.

3. Public Administration organisations making use of Generative AI tools provided through the Agent may mandate their use in any invitation to tender (ITT) or request for procurement (RFP) as well as in the contractual documents drawn up with their solution providers.
4. In case of use of alternative Generative AI tools, prior authorisation shall be sought from the respective CIO for their use for public services or information and/or advice to be given. The authorisation shall need to take into account of the intention, the consequences and the level of risk of harm of the proposed generative AI tool within the **specific context**, to:

   - the interests of the end-users of the public service or any form of advice or communication
   - the reputation and regulatory exposure of the government organisation itself.

   Further reference shall also be made to *General Statements 4 and 5 of the GMICT Centralised Digital Enabling Services Policy*.
5. Governance rules, roles and responsibilities and processes that take into account of the business impact and complexity of the proposed generative AI tool to be applied shall be clearly defined and communicated accordingly.

6. Conformance to the relevant applicable legislations, regulations, Government policies, official Public Administration communication, the AI ethical principles that are in effect and any governance rules in force, shall be expected in any activity involving the use of any Generative AI tool.

Relevant applicable legislations, include but are not limited to:

- The AI Regulation (EU) 2024/1689.
- The General Data Protection Regulation, (EU) 2016/6791 and the Data Protection Act (CAP 586) for personal data.

Human centred Accountability and Transparency

Rationale

Information provided by Generative AI tools may not often be verified, it may not be factual, and it may be unacceptably biased. Even if they are used as aids they should not act as substitutes to human decision making. Additionally, the Generative AI tools should not act as a black box, with no understanding of how results have been derived out of the data it has been trained with. A thorough understanding and ultimately, transparency with the end-user in related processing is thus necessary.

7. **Generative AI tools shall not act as the final decision maker** on any public service, or any form of advice or communication given. Any related **final decision remains vested with the individual responsible for taking it**.
8. In cases where the tools may be used to generate options, ideas or draft content, the decision-maker(s) as designated within the respective Public Administration processes, shall thoroughly **review the output,** ensuring that it:
   (i) corresponds with their understanding of the issue.
   (ii) reflects consideration of all relevant information and context.
   (iii) is in line with the end users' expectations.
   (iv) reflects conformance to relevant applicable laws, regulations, Government policies, official Public Administration communication, the AI ethical principles that are in effect and any governance rules in force.
   (v) reflects any other jurisdictional expectations of what is acceptable or otherwise in the machine learning of the tool.

   Concerns and issues related to the above are to be promptly addressed accordingly, including taking any corrective action as necessary.
9. Inaccurate or irrelevant information shall not be taken into account in such review process. If in doubt, verification with reputable sources shall be sought.
10. The capacity to explain and justify the decisions taken with respect to the public service, advice or communication given shall be ensured and maintained.
11. End-users shall be provided with clear and concise information of when their data has been used for any machine learning purposes or when it has been used by the generative AI tool as an aid for decision making.
12. Official communications shall carry a marking indicating when a generative AI tool has been used to generate their content.

Security and safety

Rationale

Precautionary measures need to be taken so as to ensure the confidentiality, integrity and availability of Government data at all times through the use of such tools.

13. A business impact assessment shall be conducted prior to the deployment of an alternative generative AI tool so as to ensure that no additional points of failure are introduced.
14. AI dependencies shall be identified and recorded so that rectifications can be effectively implemented should issues arise in the operations of a generative AI tool.
15. Reliance upon information provided by generative AI tools, in support of time-sensitive and critical decision making, shall be avoided.
16. Where technically feasible, the ability of an alternative generative AI tool to save chat history between the end-user and the tool for machine learning purposes shall be disabled.
17. Links or files generated by an alternative generative AI tool are to be assessed for malicious code in terms of policy requirements as stated within the *GMICT P0016 Information Security Policy*.
18. Fine-tuning or customisation of generative AI tools to reduce risks of data leaks through prompts shall be applied for their use.
19. Further reference shall be made to GMICT *P0016 Information Security Policy* with respect to security of all generative AI tools and of Government data.

Confidentiality of Data

Rationale

Further precautionary measures need to be kept in view especially with respect to confidentiality of Government data through the use of such tools.

20. Government data carrying security marking that is *Restricted* or higher, in line with *GMICT P 0016 Information Security policy* **shall not** be used in ***alternative*** generative AI tools.
21. Government data carrying security marking that is *Confidential* or higher, in line with *GMICT P 0016 Information Security policy* **shall not** be used in ***any*** generative AI tool.
22. The risk of input of Government data that may allow a generative AI tool to infer sensitive information, based upon aggregation of its content over time, shall be avoided.

Responsible Innovation

Rationale

Responsible innovation is a key principle for trustworthy and responsible AI. Apart from innovation, related research and development needs to be encouraged, have a clearly defined purpose, be non-biased, be ethics based, and be well-managed.

23. Public funded Research, Development and Innovation (RDI) investments, involving generative AI tools shall be defined upon outcome-based goals so as to foster creativity in the attainment of such goals.
24. Where applicable, regulatory sandboxes shall be used to test related innovations on a societal scale with safeguards that are grounded on the applicable ethical AI principles.
25. Resilience capabilities shall be taken into account and embedded, as from the initial stages of innovations related to application of Generative AI tools.

Complaints handling

Rationale

As stated earlier, for reasons of transparency, end-users of any public service or any form of advice or communication given need to be made aware of the use of their data to train the Generative AI tools or such data has been subject to the tools as an aid for decision making, They should therefore also have the possibility to request clarifications, to object or raise complaints in what they may see as infringements upon their rights and requirements. Most importantly, the response should be one that is not addressed by AI means such as a chatbot but from a purely human intervention.

26. **Recourse** options available to end-users that may allow them to challenge outcome(s) resulting from a Generative AI tool applied shall be ensured. The options shall ensure that such challenges are **appropriately** handled, remediated and responded to.

Appendix 1: Terms of Use of Microsoft 365 Copilot

1. In addition to the above GMICT Policy statements, the user shall comply with these Terms of Use, as may be updated from time to time.
2. Prior to using Microsoft 365 Copilot, the user shall complete designated training to ensure an adequate level of AI literacy. The level of training shall be proportionate to the user's role, technical knowledge, and the context in which Microsoft 365 Copilot is to be used, in accordance with Article 4(5) of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). The user's organisation shall maintain records of user training and AI literacy levels as part of its AI governance obligations.
3. The user shall comply with the Microsoft 365 Copilot Product Terms as found at https://www.microsoft.com/en-au/servicesagreement#serviceslist. The user shall familiarise with any material updates communicated by Microsoft and the Agent, that may affect the use of the Microsoft 365 Copilot license.
4. The user shall remain exclusively responsible for reviewing, verifying and validating any output or results generated by Microsoft 365 Copilot. The user acknowledges that outputs or results generated may contain inaccurate or outdated information.
5. The user acknowledges that the use of any output or results of Microsoft 365 Copilot shall be within the user's discretion, yet the user shall remain exclusively responsible and subject to any applicable internal or GMICT policy, regulations and legislation.
6. The user shall not use Microsoft 365 Copilot in a manner that results in deployment of prohibited AI practices or in a context that qualifies as a high-risk practice as defined in the Artificial Intelligence Act (Regulation (EU) 2024/1689) unless such use has been expressly authorised and all legal, technical and organizational safeguards are in place.
7. The use of Microsoft 365 Copilot may be monitored for compliance, quality assurance and audit purposes. The user consents to such monitoring and shall cooperate with any reviews or investigations related to the use of Microsoft 365 Copilot.
8. The user acknowledges and agrees that any breach of these Terms of Use may result in appropriate action by the Agent which may include, but is not limited to, suspension or revocation of access to Microsoft 365 Copilot.

Deviations from GMICT Policy

Instances where it may not be technically possible or cost-effective to comply with a particular GMICT Policy requirement shall be reported as risks to be assessed.

Breaches of GMICT Policy shall be brought to the attention of the respective CIO office in order to determine appropriate corrective action and potential control improvements involving relevant stakeholders, as appropriate.

Issuing Authority

This document has been issued by the **Principal Permanent Secretary**.

Contact Information

Government ICT Policies may be found at **http://ictpolicies.gov.mt**.

Any suggestions, queries or requests for clarification regarding Government ICT Policies may be forwarded to **ictpolicies@gov.mt**.