

人工智慧使用指引與合規規範

原子與分子科學研究所 AI 發展小組 (ATOMS)

中央研究院 原子與分子科學研究所

版本 1.0 | 2026 年 4 月 7 日

一、目的與適用範圍

本指引旨在建立原子與分子科學研究所（以下簡稱「原分所」）人工智慧（AI）工具與系統之負責任使用標準。AI 工具係作為輔助工具，不改變研究人員或職員之既有責任。本指引依據我國《人工智慧基本法》（2026 年 1 月生效）、中央研究院「使用生成式 AI 之參考指引」（2026 年 2 月）及國際學術研究 AI 使用最佳實踐制定。

適用範圍：本指引適用於原分所全體人員，包括研究人員、博士後研究員、研究生、研究助理、行政人員及訪問學者，涵蓋研究與行政活動。

二、法規架構

我國《人工智慧基本法》（2026 年）：確立七大基本原則——永續發展與福祉、人類自主、隱私保護與資料治理、資安與安全、透明與可解釋、公平與不歧視、問責。要求政府機關進行風險評估，並於 12 個月內建立內部 AI 使用規範。¹

中央研究院生成式 AI 使用指引：三大核心準則——確保 AI 生成內容之正確性、維護個人隱私與資訊安全、實踐研究透明性與課責性。²

國際標準：遵循 COPE（出版倫理委員會）、ALLEA 歐洲研究誠信行為準則，以及各期刊出版社之 AI 使用政策。^{3,4}

三、指導原則

- 正確性與品質管控** — 所有 AI 產出須經人工使用者驗證，不得未經獨立查核即採用 AI 產出。
- 隱私保護與資訊安全** — 機密、敏感或個人資料不得輸入外部 AI 系統。須遵守我國《個人資料保護法》（PDPA）。
- 透明與揭露** — 研究或行政流程中實質使用 AI 須依機構及出版社規定進行記錄與揭露。

4. 問責與責任 — 研究人員及職員對所有 AI 輔助產出負完全責任。AI 系統不得列為作者或負責人。

5. 公平與不歧視 — 使用 AI 工具時應避免在研究設計、資料分析及行政決策中產生偏見、歧視或不公正結果。

6. 資安與安全 — 涉及敏感任務時應使用經機構核准或審查之 AI 工具。使用前須評估 AI 平台之安全性。

7. 研究誠信與倫理 — AI 使用須符合既有研究倫理標準。透過 AI 工具進行造假、竄改或抄襲，構成研究不端行為。

四、許可與限制使用範圍

研究人員及職員對所有產出負完全責任。以下範例僅供參考。

4.1 研究活動

類別	範例	要求
許可使用		
許可	文獻搜尋與摘要整理	無特殊要求
許可	語言編輯與文法修潤	如實質使用須致謝
許可	程式碼除錯與優化	須驗證產出
許可	資料視覺化排版	須驗證正確性
許可	腦力激盪與構想發想	無特殊要求
許可	翻譯輔助	須驗證正確性
限制使用 (須揭露)		
限制	稿件撰寫輔助	須揭露；研究人員負完全責任
限制	統計分析與資料詮釋支援	須揭露方法；須獨立驗證
限制	圖表與插圖生成	須揭露；須驗證科學正確性
限制	研究計畫撰寫輔助	須依補助機關政策揭露
禁止使用		
捏造或竄改實驗數據或結果		

- 未揭露即將 AI 生成文字作為原創作品提交
- 於機密性同儕審查或計畫審查中使用 AI 工具
- 將未發表之研究資料、病患資料或專有資料輸入外部 AI
- 未經人工監督即使用 AI 進行人事相關自動化決策

4.2 行政活動

類別	範例	要求
許可使用		
許可	例行公文草擬	標準作業
許可	文件排版與範本製作	標準作業
許可	行政文件翻譯	須驗證正確性
許可	會議紀要草擬	分發前須核實
限制使用 (須核准)		
限制	處理含人事資料之文件	僅限使用經核准工具；不得輸入外部 AI
限制	財務文件編製	所有數字須核實；僅限使用機構工具
禁止使用		
• 人事考核、聘用或晉升之自動化決策 • 將機密或保密性機構資料輸入外部 AI 系統 • 未經人工審核與核准即使用 AI 生成機構正式聲明		

五、資料保護與資訊安全

- 不得將機密、保密或敏感之研究資料輸入外部 AI 平台。
- 不得將未發表之稿件、原始實驗數據或專有方法與 AI 系統分享。
- 個人資料 (姓名、身分證字號、健康資料) 除使用經機構核准之安全平台外，不得輸入 AI 工具。
- 使用雲端 AI 服務時，須確認服務提供者之資料處理及隱私政策。

- 優先使用機構認可之 AI 工具（例如：具有資料保護協議之企業版本）。
- 於使用 AI 工具處理敏感資訊之前，須進行風險評估。
- 保存 AI 工具使用紀錄，以備稽核與合規之用。

六、研究誠信與出版規範

- 投稿前應遵循各期刊之 AI 揭露政策（請查閱 COPE、Nature、Science、Elsevier、IEEE 等規定）。
- AI 系統不得列為任何出版品之作者——著作權要求 AI 無法履行之課責性。
- 稿件中所有 AI 生成之內容，須於研究方法或致謝段落中揭露。
- 研究人員須獨立驗證所有 AI 生成之引用文獻、參考資料、數據及事實陳述。
- 保存 AI 提示詞、使用之工具（名稱、版本）及使用日期之文件紀錄，以利再現性。
- AI 輔助之分析須具可再現性；應充分記錄流程以供獨立驗證。
- 於同儕審查及研究計畫評審中，不得將稿件或計畫內容輸入 AI 工具，以保護機密性。

七、自主與代理式人工智慧系統

自主與代理式 AI 系統在歸屬問責與責任方面可能帶來挑戰。啟動或操作代理式或自主 AI 系統之研究人員及職員，對該等系統之行為負最終責任。此類系統之使用須具備適當之安全防護措施與監控機制，以防止發生非預期或失控之結果。如研究人員或職員對操作自主或代理式系統可能產生意外結果感到疑慮，鼓勵其主動與 ATOMS 工作小組及資訊安全部門討論其系統。

八、合規與執行

- 所長指定**原子與分子科學研究所 AI 發展小組 (ATOMS)**負責監督執行。
- 本指引將定期檢視並視需要更新；如法規變動則提前修訂。
- 原分所應為所有新進人員提供負責任 AI 使用之訓練與說明(**經由 ATOMS AI Literacy Group 執行**)。
- 人員發現 AI 濫用或違規情事，應循機構管道通報(**原分所行政委員會及/或學術委員會**)。
- 違規者依中央研究院相關規定及適用法律予以處分。
- 現行機構合規、稽核及通報機制，於涉及 AI 相關活動時同樣適用。
- 凡合規、透明度或再現性有所需要，應依機構及外部要求保存 AI 工具使用紀錄（**經由各實驗室及行政單位執行**）。

八、參考文獻

1. 《人工智慧基本法》，2026 年 1 月 14 日生效。 <https://law.nstc.gov.tw/LawContent.aspx?id=GL000592>
2. 中央研究院「使用生成式 AI 工具之參考指引」，2026 年 2 月。
https://www.ias.sinica.edu.tw/storage/upload/ck_files/Guidelines_for_Using_Generative_AI_Tools.pdf
3. 歐盟執行委員會「生成式 AI 於研究之負責任使用：實踐指引」，2026 年。 https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en
4. COPE「AI 工具與著作權立場聲明」，2023 年。 <https://publicationethics.org/cope-position-statements/ai-author>

IAMS AI Guideline and Compliance

AI-Task Force on Molecular Sciences (ATOMS)

Institute of Atomic and Molecular Sciences (IAMS)

Academia Sinica, Taiwan

Version 1.0 | April 8, 2026

1. Purpose and Scope

Purpose: This guideline clarifies how existing standards for responsible research and administrative practice apply to the use of artificial intelligence (AI) tools at IAMS. AI tools are treated as assistive tools that do not alter the responsibilities of researchers or staff. It aligns with Taiwan's AI Basic Act (effective January 2026), Academia Sinica's Guidelines for Using Generative AI Tools (February 2026), and international best practices for AI in academic research.

Scope: This guideline applies to all IAMS personnel — including research fellows, postdoctoral researchers, graduate students, research assistants, administrative staff, and visiting scholars — in both research and administrative activities.

2. Regulatory Framework

Taiwan AI Basic Act (2026): Establishes seven fundamental principles — sustainable development, human autonomy, privacy protection, cybersecurity, transparency, fairness, and accountability. Requires government entities to conduct risk assessments and establish internal AI use rules within 12 months.¹

Academia Sinica Generative AI Guidelines: Three core principles — accuracy of AI-generated content, privacy and information security, and research transparency and accountability.²

International Standards: Alignment with COPE (Committee on Publication Ethics), ALLEA European Code of Conduct for Research Integrity, and publisher-specific AI policies (Nature, Science, Elsevier, Wiley, IEEE).^{3,4}

3. Guiding Principles

1. Accuracy and Quality Control — All AI-generated outputs must be verified by human users. Researchers shall not rely on AI outputs without independent validation.

2. Privacy Protection and Data Security — Confidential, sensitive, or personal data shall not be input into external AI systems. Compliance with Taiwan's Personal Data Protection Act (PDPA) is mandatory.

3. Transparency and Disclosure — Substantial use of AI in research or administrative processes must be documented and disclosed in accordance with institutional and publisher requirements.

4. Accountability and Responsibility — Researchers and staff bear full responsibility for all outputs produced with AI assistance. AI systems cannot be designated as authors or responsible parties.

5. Fairness and Non-Discrimination — AI tools shall be used in ways that avoid bias, discrimination, or inequitable outcomes in research design, data analysis, and administrative decisions.

6. Cybersecurity and Safety — Only institutionally approved or vetted AI tools shall be used for sensitive tasks. Personnel must assess the security posture of AI platforms before use.

7. Research Integrity and Ethics — AI use must comply with established research ethics standards. Fabrication, falsification, or plagiarism through AI tools constitutes research misconduct.

4. Permitted and Restricted Uses

4.1 Research Activities

Category	Examples	Requirements
Permitted Uses		
Permitted	Literature search and summarization	No special requirement
Permitted	Language editing and grammar polishing	Acknowledge if substantial
Permitted	Code debugging and optimization	Verify outputs
Permitted	Data visualization formatting	Verify accuracy
Permitted	Brainstorming and idea generation	No special requirement
Permitted	Translation assistance	Verify accuracy
Restricted Uses (Require Disclosure)		
Restricted	Manuscript drafting assistance	Must disclose; researcher retains full responsibility
Restricted	Statistical analysis and data interpretation support	Must disclose method; verify independently
Restricted	Figure and illustration generation	Must disclose; verify scientific accuracy
Restricted	Grant proposal writing assistance	Must disclose per funder policy
Prohibited Uses		
• Fabricating or falsifying experimental data or results • Submitting AI-generated text as original work without disclosure • Using AI tools during confidential peer review or proposal evaluation • Inputting unpublished research data, patient data, or proprietary data into external AI • Using AI for automated decisions on personnel matters without human oversight		

4.2 Administrative Activities

Category	Examples	Requirements
Permitted Uses		
Permitted	Drafting routine communications	Standard practice
Permitted	Document formatting and template creation	Standard practice

Permitted	Translation of administrative documents	Verify accuracy
Permitted	Meeting summary drafting	Verify before distribution
<i>Restricted Uses (Require Approval)</i>		
Restricted	Processing documents containing personnel data	Use approved tools only; do not input into external AI
Restricted	Financial document preparation	Verify all figures; institutional tools only
<i>Prohibited Uses</i>		
• Automated decision-making on personnel evaluations, hiring, or promotions • Inputting classified or confidential institutional data into external AI systems • Using AI to generate official institutional statements without human review and approval		

5. Data Protection and Information Security

- Do not input classified, confidential, or sensitive research data into external AI platforms.
- Do not share unpublished manuscripts, raw experimental data, or proprietary methodologies with AI systems.
- Personal data (names, ID numbers, health data) must never be entered into AI tools unless using institutionally approved, secure platforms.
- When using cloud-based AI services, verify the provider's data handling and privacy policies.
- Use institutionally sanctioned AI tools when available (e.g., enterprise versions with data protection agreements).
- Conduct a risk assessment before adopting new AI tools for tasks involving sensitive information.
- Maintain records of AI tool usage for audit and compliance purposes.

6. Research Integrity and Publication

- Follow journal-specific AI disclosure policies before submission (check COPE, *Nature*, *Science*, *Elsevier*, *IEEE*, etc.).
- AI systems shall not be listed as authors on any publication — authorship requires accountability that AI cannot fulfill.
- All AI-generated content in manuscripts must be disclosed in the methods section or acknowledgments.
- Researchers must independently verify all AI-generated citations, references, data, and factual claims.
- Maintain documentation of AI prompts, tools used (name, version), and dates of use for reproducibility.
- AI-assisted analyses must be reproducible; document the process sufficiently for independent verification.
- During peer review and grant evaluation, do not input manuscript or proposal content into AI tools to protect confidentiality.

7. Autonomous and Agentic Systems

Autonomous and agentic AI systems can pose challenges in attributing accountability and responsibility. Researchers and staff who initiate or operate agentic or autonomous AI systems retain ultimate responsibility for the actions of these systems. Such systems shall be used with appropriate safeguards and monitoring to prevent unintended or uncontrolled outcomes. Researchers and staff who are concerned about the potential for unexpected outcomes from operating autonomous or agentic systems are encouraged to discuss their system with the ATOMS Task Force and IT Security.

8. Compliance and Implementation

- The IAMS Director has designated the **AI-Task Force for Molecular Sciences (ATOMS, IAMS, AS)** to oversee implementation.
- This guideline will be periodically reviewed and updated as needed.
- IAMS shall provide training and orientation on responsible AI use for all new personnel (**via the ATOMS AI Literacy Group**).
- Personnel who become aware of AI misuse or compliance violations should report through institutional channels (**IAMS Administrative Committee and/or Academic Committee**).
- Non-compliance may be subject to disciplinary measures in accordance with Academia Sinica regulations and applicable laws.
- Existing institutional compliance, audit, and reporting mechanisms apply to AI-related activities where relevant.
- Where required for compliance, transparency, or reproducibility, records of AI tool use should be maintained in accordance with institutional and external requirements (via respective labs and administrative units).

8. References

1. Artificial Intelligence Basic Act, Taiwan (人工智慧基本法), effective January 14, 2026. <https://law.nstc.gov.tw/LawContent.aspx?id=GL000592>
2. Academia Sinica, "Guidelines for Using Generative AI Tools," February 2026. https://www.ias.sinica.edu.tw/storage/upload/ck_files/Guidelines_for_Using_Generative_AI_Tools.pdf
3. European Commission, "Responsible Use of Generative AI in Research: Living Guidelines," 2026. https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en
4. COPE Council, "COPE Position Statement on Authorship and AI Tools," 2023. <https://publicationethics.org/cope-position-statements/ai-author>