

國軍使用生成式 AI 服務平臺作法

- 一、因應生成式 AI 服務平臺係運用大量蒐集、學習用戶提供資訊產出各式成品，使用不慎恐涉及軍事機密、個資安全及侵害智慧財產權等疑慮，為確保資訊安全，訂定本作法。
- 二、國軍以軍事安全為首要，為防資料遭蒐集學習記錄，凡屬國軍公務資訊或其他法規所限制之資訊及個資，嚴禁發布上傳至任何生成式 AI 服務平臺，並不得藉此平臺製作或處理各類業管公務文書。
- 三、生成式 AI 服務平臺有可能產出不正確或模糊之資訊，官兵於個人查詢參考使用前須仔細查核比對驗證，以維資料準確性。
- 四、嚴禁利用各類生成式 AI 服務平臺從事非法及違反社會善良風俗之活動，若涉及國防機密外洩或損害國軍軍譽者，依法究辦。
- 五、官兵個人運用生成式 AI 服務平臺於進修教育及終生學習等面向時，應遵守資通安全、個資保護、著作權與相關學術倫理規範，並注意其侵害智慧財產權之可能性。
- 六、各單位應就所辦採購事項，要求得標之法人、團體或個人注意本作法，並遵守相關規範。
- 七、各單位得參照本作法，訂定所屬使用生成式 AI 服務平臺之規範。