



UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CALIFORNIA 92278-8100

5231
G-3/5

MAR 04 2026

POLICY LETTER 2-26

From: Commanding General
To: Distribution List

Subj: MARINE AIR GROUND TASK FORCE TRAINING COMMAND ARTIFICIAL INTELLIGENCE
POLICY

Ref: (a) U.S. DOD RESPONSIBLE AI STRATEGY
(b) NAVMC 5239.1, USMC GUIDANCE ON GenAI

1. Guiding Principles

a. All Artificial Intelligence (AI) capabilities used and developed by this command will be consistent with the DoD AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, and Governable per reference (a).

b. System users bear sole responsibility for their input and acceptance of output from Generative AI (GenAI) tools. Users are responsible for products and decisions made with the assistance of GenAI.

c. Because AI tools can produce results that appear genuine but are in fact inaccurate, misleading, or false, users must verify outputs from AI systems for accuracy and appropriateness prior to acceptance or use.

d. AI-generated products must be appropriately identified. Presenting AI-generated content as exclusively human-created without proper attribution is prohibited. Users will label any document that was created, in whole or in part, with outputs from GenAI tools, using their best judgment on whether specific citations are needed based on the importance of transparency.

2. Acceptable Use of GenAI

a. GenAI is authorized for professional use by all Marine Air Ground Task Force Training Center (MAGTFTC) personnel. Examples of acceptable use include:

- (1) Brainstorming.
- (2) Drafting communications.
- (3) Conducting research.
- (4) Improving code.
- (5) Assisting with translation.
- (6) Summarization of documents.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

POLICY LETTER 2-26

(7) Creating rough drafts of presentations.

(8) Generating images for illustrative purposes in unclassified products.

(9) Generating training scenarios and student handouts.

b. The use of GenAI is prohibited for the following purposes:

(1) Generating or disseminating official Marine Corps endorsements of commercial products or services.

(2) Generating or disseminating content that violates copyright laws or intellectual property rights.

(3) Generating or disseminating content that is discriminatory, harassing, offensive, libelous, defamatory, or otherwise unlawful.

(4) Generating or disseminating "deepfakes" or other intentionally deceptive or misleading content that could harm individuals, organizations, or the integrity of official information.

(5) Making decisions that could have a significant impact on individuals or organizations without human review and validation.

(6) Using GenAI to support critical functions without ensuring qualified personnel validate all outputs and maintain operational control.

(7) Circumventing existing security controls or access restrictions.

3. Data Security and Privacy

a. Workflow Use

(1) All personnel are responsible for the information they input into GenAI systems and must adhere to existing legal, cybersecurity, information, operational security, and classification policies. The use of proprietary, sensitive, or classified information in commercial or public-facing generative AI models is prohibited.

(2) All data used for GenAI systems must comply with all applicable privacy regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), and the Privacy Act.

(3) Prior to use in GenAI systems, data will be de-identified or anonymized to minimize the risk of privacy violations, using techniques approved by the MAGTFTC/MCAGCC Data Steward where applicable.

b. GenAI Projects

(1) GenAI projects will prevent unauthorized transmission of sensitive data to GenAI systems through:

(a) User training on data handling requirements.

POLICY LETTER 2-26

(b) Use of DOD-accredited GenAI platforms (e.g., GenAI.mil), with appropriate data classifications.

(c) Monitoring and enforcement of data input policies.

(d) Implementation of technical controls where available.

(2) All GenAI systems that collect, use, or disclose personal information must undergo a privacy impact assessment.

(3) Maintenance and disposal of equipment hosting GenAI systems requires the assistance of the Data Steward to prevent future data vulnerabilities.

4. Governance and Risk Management. Commands are discouraged from banning the use of GenAI tools. Instead, commands will develop and maintain appropriate governance processes that holistically weigh the benefits of AI tools against potential risks and ensure their use supports organizational objectives while maintaining security and integrity.


M. H. CLINGAN

DISTRIBUTION: A