STATE OF CALIFORNIA – MILITARY DEPARTMENT
HEADQUARTERS, CALIFORNIA CADET CORPS
Camp San Luis Obispo
10 Sonoma Ave, Bldg. 1301
Camp San Luis Obispo, California 93405

CACC-HQ-CO 20 June 2025

LETTER OF INSTRUCTION 010-2526-001

Responsible Data and Personally Identifiable Information (PII) Handling

1. PURPOSE: This letter of instruction establishes policy and procedures for the proper handling, protection, and transmission of Personally Identifiable Information (PII) within the California Cadet Corps. As a youth military leadership program under the California Military Department (CMD), we have a heightened obligation to protect the privacy of minors and their families.

2. REFERENCES:

    a. California Government Code § 11019.9 – *Protection of Information on Individuals*
    b. State Administrative Manual (SAM) Sections 5300–5399 – *Information Security*
    c. California Military Department (CMD) Information Security Policy, latest edition
    d. California Education Code § 49073.1 – *Use and Protection of Pupil Records*

3. POLICY: All California Cadet Corps personnel, both adult and Cadet, are expected to handle PII with the highest level of care. Improper handling or sharing of such information may compromise the safety of Cadet participants and expose the organization to liability.

4. DEFINITIONS:

    a. *Personally Identifiable Information (PII):* Information that can be used to distinguish or trace an individual's identity, including but not limited to: full names, home addresses, email addresses, phone numbers, dates of birth, Social Security Numbers, student IDs, and parent/guardian contact information.
    b. *Cadet Data:* PII pertaining to Cadets under the age of 18, as well as those 18 years or older who remain enrolled in the program as students. This includes, but is not limited to, medical information, academic records, and any data that may reveal a cadet's identity, location, or other sensitive personal details.
    c. *Spillage:* The unauthorized disclosure, transmission, or exposure of sensitive or protected data.

5. PROHIBITED ACTIVITES: The following actions are strictly forbidden:

    a. Posting or sharing PII or group rosters in any digital or physical format accessible to the public or unauthorized personnel.
    b. Transmitting PII via messaging applications, social media, or otherwise unofficial means without prior approval from the S6 or designated Information Officer.

c. Sharing phone numbers, email addresses, home addresses, or other personal information of Cadets, staff, or volunteers with third parties without a demonstrated need-to-know and consent.
d. Using personal cloud storage or unsecured devices to store or process Cadet data.
e. Printing documents containing PII in public locations, or leaving such documents unsecured.

6. AUTHORIZED USES: PII may only be accessed or transmitted:

a. By individuals who have completed annual data protection training and who have a verified need-to-know.
b. Through secure and approved systems that comply with CMD and State of California security policies.
c. When prior written consent from a parent or guardian has been obtained for release of Cadet-related data.

7. CADET PRIVACY EMPHASIS: All adult staff must exercise extreme caution when handling Cadet records, including but not limited to emergency contact forms, medical information, or school performance data. Under no circumstances should a Cadet's location, schedule, or contact information be released to non-program personnel or peers.

8. TRAINING AND ACCOUNTABILITY: Designated adult personnel that handle PII must complete annual PII and data handling training. The S6 section will maintain compliance records. Annually required PII training is available at the following link: https://securityawareness.dcsa.mil/piiv2/index.htm. All designated personnel must complete the training and submit a valid certificate of completion within 60 days of the LOI publication date. Failure to complete required training may result in loss of access.

9. INCIDENT REPORTING: Suspected or confirmed data breaches or spillage must be reported within 24 hours to the S6. A written incident report will be required for follow-up and mitigation.

10. ENFORCEMENT: Violation of this LOI may result in administrative action, removal from leadership or volunteer roles, and referral to higher command or legal authorities as appropriate.

11. POINT OF CONTACT: The point of contact for this LOI is 1LT Andrew Roach, HQCACC S6, andrew.roach@cacadets.org.

COL (CACC)
Michael J. Smith
Digitally signed by COL (CACC) Michael J. Smith
Date: 2025.06.22 14:35:22 -07'00'

MICHAEL J. SMITH
COL, CACC
Commanding