By signing this document, you acknowledge and consent to the following rules of conduct and policies when accessing the United States Military Academy (USMA) network, to include the Internet:

1. In Accordance With (IAW) Army Regulation (AR) 25-2 para 4-5m(7), "YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential." See also United States Corps of Cadets (USCC) Regulations and policies, USMA Regulations and policies, Army Regulation (AR) 25-1, AR25-2, the Joint Ethics Regulation and the USMA Acceptable Use Addendum. In general these references remind users to do nothing that is illegal, immoral, or unethical.
2. This paragraph applies to USMA's Cadets. Cadets' class-specific laptops, accessories, and tablets bought by cadets are personal equipment that USMA authorizes to connect to USMA's Defense Research and Engineering Network (DREN). The authorization has several conditions:
    a. USMA registers the device; where feasible (e.g., laptop), the device must use a USMA provided IS 'image,'; USMA retains remote administrative rights and prerogatives to such systems while the cadet is enrolled at USMA; formal exceptions to Army policies regarding personal equipment on USG networks.
    b. Upon cadets' graduation or separation from USMA, cadets' laptops, tables, and accessories cease to have any permission to connect to the USMA DREN. Cadets will receive an up-to-date non-government image for their laptop prior to their departure from West Point.
3. There is no blanket authorization to connect personal equipment (e.g., gaming systems, phones, computers, tablets) to the DREN. USMA provides exceptions to policy and other authorizations when requested through chains of command to the CIO/G6 and approved by the CIO/G6 or Superintendent.
4. You acknowledge that in the event of a classified information spillage, the system(s) with the classified data are subject to seizure and, as feasible, forensic wiping to remove the classified data and return, as feasible, of the sanitized device(s).
5. USMA will treat unauthorized devices discovered on the DREN as an active threat and will investigate and remediate. This includes devices within the physical jurisdiction of USMA that are interfering with USMA's network(s) (e.g., WiFi hotspots in barracks, other radio frequency (RF) emitters degrading USMA's use of RF for network operations).
6. You are responsible for understanding and abiding with what USMA has authorized (and not authorized) for usage/behavior. Violations of this AUP and any addendums, USMA, Army, DoD, or Joint regulations/policies, may result in consequences including: loss of network access, loss of administrative privileges on government managed system(s), loss of access to network provided service(s); civilian or military administrative action; civilian or military criminal action.

I have read the statement above and will comply accordingly.

_____ _____ _____

Printed Name/xNumber Signature Date