INTRODUCTION

All students, Faculty, and Staff are responsible for using Valley Forge Military Academy & College’s (VFMAC) information systems in an effective, efficient, ethical, and lawful manner. Inappropriate use exposes VFMAC to risks, including virus attacks, the compromise of network systems and services, and legal issues. Effective Information Technology (IT) security must be a team effort involving the participation of every employee, cadet, and affiliate who deals with information or information systems; therefore, these rules are in place to protect both the employee and VFMAC. The use of information systems is a privilege, not a right. This privilege will be revoked at any time for misuse.

1. **Scope** – This policy applies to employees, students, contractors, consultants, temporary employees, and other workers at VFMAC, including all personnel affiliated with third parties. It applies to all equipment that is owned or leased by VFMAC. The following provisions apply to the use of any and all IT systems used by, used on, or associated with, VFMAC:
   a) All access to information system will be authorized only through the Information Systems Department.
   b) Computers will be used only for the purpose of academic or other authorized activities.
   c) Information systems will not be used for commercial purposes or non-school-related activities.
   d) Users will not attempt to monitor another user’s activity or delete files residing on any machine other than their own.
   e) Fraudulent, harassing, threatening, libelous, obscene, pornographic, religiously offensive, and other inappropriate materials or messages will not be emailed, printed, requested, displayed, uploaded, downloaded, or stored.
   f) Information systems will not be used in any manner which may constitute criminal activity.
   g) Hacking and attempting to gain unauthorized access and/or rights to information systems is not permitted.

2. **Internet and Email:**
   a) Chain letter creation or participation, random distribution, spamming, and other forms of mass e-mailing are prohibited.
   b) Use of e-mail for personal financial gain is prohibited.
   c) Transmitting and receiving e-mail to and from friends, family, faculty, and staff is permitted.
   d) E-mail professionalism dictates that all email contains a subject line and all capital letters not be used. Users should be polite and not use profanity or vulgarity.
   e) Copying information verbatim from the Internet into homework assignments constitutes plagiarism, which is prohibited.
   f) Goods and services may be purchased through the Internet if they are categorized as acceptable by VFMAC Code of Ethics.
   g) Chat rooms and Internet games are not considered educational use of the Internet.
   h) Activities such as these impede performance of Internet bandwidth and are prohibited unless they are part of a class activity or specific assignment.
3. **Network Resources:**
   a) Software, such as multi-user games, that relies on any Valley Forge Military Academy & College network will not be installed on any computer system on campus unless deemed necessary and approved by the Department of Information Technology.
   b) Computer games will not be played on VFMAC owned computers, unless as part of an academic program.
   c) Peer to peer sharing of any computer information through any VFMAC network is permitted, but not encouraged, as it degrades network performance. Information should be exchanged through Internet mail.
   d) No user may deliberately attempt to degrade the performance of any computer system. This is directed toward, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms. Activity of this nature is considered vandalism.
   e) Network traffic routed through the Internet is subject to any acceptable use policies through which it flows, as well as to the policies in this document.
   f) **College cadets** are permitted to use Mobile Internet Devices on campus.
   g) Personal routers are not allowed in Barracks.
   h) College Cadets are afforded 24-hour Internet services while Academy Cadet Internet services are disabled between 22:00 and 5:30 [M – F].

4. **Security Issues**
   a) If any user discovers faults in system security, it is their responsibility to bring it to the attention of the Information Systems Department immediately.
   b) Any copyrighted software is not to be copied to or from any VFMAC computer.
   c) A computer, computer account, user password, or e-mail account assigned to an individual will not be used by others. If a user feels that knowledge of their password has been obtained by others or otherwise compromised, they should change their password.
   d) Users may apply password protection, file encryption, and other devices for security, but will not attempt to deprive authorized personnel of any necessary access.
   e) Network access to any Faculty or Staff computer is strictly prohibited unless authorized by appropriate Information Systems personnel. (Major)
   f) Users will not attempt to circumvent system security or disguise themselves or their machine identity for any reason. A user will not change their computer/Internet address or network configuration. (Major)
   g) Users must log in to their computer when working and log out when finished. Leaving a machine logged in could allow someone else to make use of unauthorized network resources.

5. **Disciplinary Issues** – Computer Policy violations are considered as either minor or major.
   a) Violations of this policy will be handled in accordance with Valley Forge Military Academy & College policies and may result in disciplinary action, to include, but not limited to the restriction of network access, loss of network privileges, dismissal from Valley Forge Military Academy & College and legal action.
   b) Violations of the above policies may constitute a criminal offense punishable under Pennsylvania or United States Federal law. As an example, under Pennsylvania law, “…it is a felony punishable by fine up to $15,000 and imprisonment up to seven years for any person to access, alter, or damage any computer system, network, software, database, or any part thereof, with the intent to interrupt the normal functioning of an organization (18Pa.C.C.3933(a)(1))…” “…Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software (18 Pa.C.S.3933(a)(2) and (3))…”
c) During the six-week indoctrination period known as the Plebe System, Plebes may use computers for academic purposes during Evening Study Hall, which is conducted from 1930 to 2130 hours Sunday through Thursday. Plebes are allowed to use a computer for academic purposes outside Evening Study Hall; however, they must obtain permission from their Tactical Officer to do so. Computers will not be used for e-mail or instant messaging during the Plebe System.

6. **Minor and Major Offenses:**
   
   a) **Minor Offense:**
      
      i. Unauthorized computer use during Plebe System. [see paragraph (5) (c) above]
      
      ii. Use of the network computing for product advertisement or political lobbying.
      
      iii. Accessing obscene or pornographic materials.
      
      iv. Accessing prohibited social networking websites from network or personal computer. Such websites include, but are not limited to, MySpace, Facebook, Xanga, Webshots, Youthink, Studentcenter, Hi5, Youtube and Friendster.
      
      v. Attaching any device other than a personal computer to the campus network without the expressed permission of the information technology staff. This includes (but is not limited to) hubs, switches, routers, and protocol analyzers.
      
      vi. Accessing another person’s computer, files or data without permission. This includes data in transit on the network.
   
   b) **Major Offense:**
      
      i. Fraudulent, harassing, threatening, libelous, obscene, pornographic, religiously offensive, and other inappropriate materials or messages may not be emailed, printed, requested, displayed, uploaded, downloaded, or stored.
      
      ii. Information systems may not be used in any manner, which may constitute criminal activity.
      
      iii. Hacking and attempting to gain unauthorized access or rights to information systems internally or outside of VFMAC.
      
      iv. No form of harassment or hateful incident will be tolerated. Incidents and practices of cyber bullying will not be tolerated. Cyber bullying involves the use of information and communication technologies, such as e-mail, cell phone and pager text messages, instant messaging, and defamatory personal Web sites, to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others.
      
      v. Transmitting materials likely to be offensive or objectionable to recipients.
      
      vi. Any material posted by a cadet on YouTube (or other video hosting sites) who brings discredit upon VFMAC or shows Valley Forge in a bad light by exhibiting poor behavior will be considered a major violation of the school’s computer policy and treated as a Class A Offense which may result in dismissal.

I have read and understand the Computer Use Policy at Valley Forge Military Academy & College:

<table>
<thead>
<tr>
<th>Cadet Signature</th>
<th>Cadet Name Printed</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Signature</td>
<td>Parent Name Printed</td>
<td>Date</td>
</tr>
</tbody>
</table>