This policy applies to all users including faculty, staff, students, and guest users of Delaware Valley College’s computer networks, equipment, or connecting resources.

**College Inspection of Personal Electronic Information** -- Electronic information on College networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by the College where:

1. It is necessary to maintain or improve the functioning of College computing resources;
2. There is a suspicion of misconduct under College policies, or suspicion of violation of Federal or State laws; or
3. It is necessary to comply with or verify compliance with Federal or State law.

**Responsibilities/Prohibited Uses**

1. **Responsibilities of Users of College Computer Resources**
   1. Compliance with all applicable laws, regulations, and University policies.
   2. Adhere to data access policies of the College or those established by law.
   3. Respect for the rights and property of others, including intellectual property rights
   4. Protect user ID, password, and system from unauthorized use
   5. Adhere to the terms of software licenses and other contracts. Persons loading software on any College computer must adhere to all licensing requirements for the software. Except where allowed by College site licenses, copying software licensed for College use for personal use is a violation of this policy.
   6. Truthfulness and honesty in personal and computer identification
   7. Use College computer resources in a manner that is compliant with College policies and State and Federal law.

2. **Prohibited Uses of College Computer Resources**
   1. Unauthorized or excessive personal use. Use may be excessive if it overburdens a network, results in substantial use of system capacity, or otherwise subjects the institution to increased costs or risks (employees additionally may be subject to discipline for unauthorized or excessive personal use of computer resources.)
   2. Uses that interfere with the proper functioning of the College's information technology resources.
   3. Uses that unreasonably interfere with the ability of others to make use of College computer resources.
   4. Attempting to gain or gaining unauthorized access to the computer system, or files of another.
5. Use of College resources to violate copyright laws and infringe on the intellectual property rights of others.

6. Use of College computing equipment to view inappropriate materials. This includes pornography and other materials that would be deemed inappropriate in an office or public setting. Using personal computing equipment in public areas to view inappropriate materials is also prohibited.

7. Use of College computer resources for personal profit.

3. Email Specific Responsibilities of Users
   1. Users should maintain their email boxes in a responsible manner. This includes deleting unwanted messages and keeping stored messages to a minimum.
   2. Be professional and careful about what you say regarding other persons.
   3. Use discretion when forwarding mail to group addresses or distribution lists.

4. Prohibited Uses of College Email
   1. Knowingly sending or forwarding of chain letters or emails that contain viruses or other malicious content is strictly prohibited.
   2. Sending harassing or other inappropriate emails.

**Enforcement and Penalties for Violation:** Any person who violates any provision of this policy, of other relevant College policies, or of applicable City, State, or Federal laws or regulations may face sanctions up to and including termination, expulsion. Depending on the nature and severity of the offense, violations can be subject to disciplinary action through the Student Disciplinary System or disciplinary procedures applicable to faculty and staff. Offenders may also be subject to criminal prosecution under federal or state law, and should expect the College to pursue such action.

It may at times be necessary for authorized systems administrators to suspend someone’s access to College computing resources immediately for violations of this policy, pending interim resolution of the situation (for example by securing a possibly compromised account and/or making the owner of an account aware in person that an activity constitutes a violation). In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.