A school computer account at ASMSA gives the user access via the school computer system to the school's academic software and the Internet. A computer account is a privilege, not a right. If a user abuses the privileges, account access could be revoked. An ASMSA computer account is maintained by responsible behavior on the part of the account holder and complying with ASMSA computer usage policies. Just because a particular activity is not expressly prohibited by the computer usage policy does not mean that it is permissible for the user to engage in it. If you are unsure whether an activity is allowed or not, contact the Network Administrator. The loss of computer/network access could have a negative impact upon a student's grade in his or her coursework. Infractions of this Computer Use Policy are classified as Tier 1, Tier 2, or Tier 3, while infractions of the Disciplinary Code are referred to as Level 1, Level 2, Level 3, Level 4, or Level 5. A violation of the Computer Use Policy may also constitute a violation of the Disciplinary Code.

1. Responsibilities

a. Students are responsible for their own actions. Students are required to participate in ensuring the legal and ethical use of the school's technology and user accounts. Any violation of these guidelines should be reported to the computer lab supervisor or to the Network Administrator.

b. Students are owners of their data, and it is their responsibility to ensure that it is adequately protected against unauthorized access. Account passwords should be kept confidential and not be shared with anyone (Tier 2 infraction).

c. Students should change their password frequently and not use their names, parents' or friends' names, or a password that can easily be guessed. Students should not allow anyone else to use their account for any reason (Tier 2 infraction).

d. Students should always log out from their account when finished and always remain aware of possible security risks while logged in (Tier 2 infraction).

e. Students should periodically perform maintenance on their account by deleting old files, including old e-mail messages.

f. The Network Administrator has authority to delete files when it is deemed necessary. Each user will normally be given adequate time to remove files from the network before deletion.

2. Classroom Use of Computers and Technology

While in classroom instruction or in a lab setting, computer and technology privileges are limited by the instructor or lab monitor. Each student is expected to use the ASMSA technology in compliance with the instructor. No use of e-mail or Internet activity is allowed unless the instructor has authorized such use in the classroom. Each academic lab may impose additional rules, not explicitly covered in this Acceptable Use Policy. Failure to comply will be considered an infraction of the Computer Use Policy (Tier 2 infraction).

3. Student Use of Technology from ASMSA Residence Hall Rooms

Students will have privacy in the residence hall rooms, but any/all complaints about abuse will be investigated. If actions occur in violation of school policy, necessary action will be taken. Inappropriate use of technology may be punishable by state and federal law and is subject to disciplinary action under ASMSA policy.

4. Unauthorized Access to Files and Directories

a. Students must not engage in any activity intended to circumvent computer security controls. They must not attempt to crack passwords, to discover unprotected files, or to decode encrypted files. This also includes creating, modifying, or executing programs that are designed to hack computer systems (Tier 3 infraction).

b. Students are prohibited from downloading, possessing, or using software designed to destroy data, provide unauthorized access to the computer system, or disrupt the computing processes in any way. Using viruses, worms, Trojan horses, or any other invasive software is expressly forbidden (Tier 3 infraction).

c. Students must not access the accounts of others with the intent to read, browse, modify, copy, or delete files and directories (Tier 3 infraction).

d. Accessing unauthorized files or accounts may be punishable by state and federal law and is subject to disciplinary action under ASMSA policy. 5. Unauthorized Use of Software.

a. Students are prohibited from placing or installing any software (executables) on any ASMSA computer system without approval from the Network Administrator. This includes commercial, shareware, and freeware software. Students are expressly prohibited from using ASMSA computers to make illegal copies of licensed or copyrighted material. Some examples of material that may be copyrighted are intellectual property, clip art, images, photo, sound, as well as software packages. Copyrighted material must only be used in accordance with its license or purchase agreement. Students do not have the right to possess or use unauthorized copies of materials or to make unauthorized copies for themselves or anyone else (Tier 2 infraction).

b. ASMSA has installed anti-virus software on many of its computer systems. Students are prohibited from tampering with this software or turning it off, which could allow the network to become infected (Tier 2 infraction).
c. Unauthorized use of software may be punishable by state law.

6. Use For-Profit Activities
The school's computer systems are for the sole use of the school. Students are prohibited from using the school's computers for personal financial gain, unless specifically authorized by the Director (Tier 2 infraction).

7. Electronic Mail (E-mail)
a. The ASMSA e-mail system is provided for educational purposes and as a means to widen the communication channels between students, faculty, staff, and administration. No means is provided for private e-mail when using the ASMSA mail system. The ASMSA faculty/staff reserve the right to intercept, detain, and read both incoming and outgoing e-mail from the ASMSA mail system. There is no guarantee of privacy when using the ASMSA mail system, as all ASMSA mail is subject to public disclosure and scrutiny.
b. Students are prohibited from transmitting or forwarding fraudulent, harassing, obscene, or inappropriate messages and files. Students must not send any electronic mail or other form of electronic communication by forging another's identity or attempting to conceal the origin of the message in any way. (Tier 2 infraction).
c. Students are prohibited from transmitting or forwarding chain letters, mass mailings, or SPAMing of mail systems or of individual users. (Tier 2 infraction).
d. Students may not access or attempt to access another person’s e-mail. (Tier 2 infraction).
e. Using e-mail without permission during class time is a Tier 1 infraction for the first offense, and a Tier 2 infraction for all subsequent offenses.

8. Network Communications
a. Remote communications (i.e., ASMSA provided e-mail and ASMSA provided Internet access) are provided only for educational purposes. Any attempt to gain unauthorized access to either ASMSA computers or to remote computers is strictly prohibited. Such attempts are illegal and subject to prosecution (Tier 3 infraction).
b. Playing computer games and recreational computing (MUDDing, BBSing, etc.) are not allowed in the academic labs, the library, or classrooms (Tier 2 infraction).
c. The use of computers and networks to download, upload, create, reproduce, and/or distribute files containing vulgar language and/or obscene material is prohibited (Tier 2 infraction).
d. Users of electronic communication facilities such as e-mail, bulletin boards, and news groups are obligated to comply with the restrictions and acceptable practices established for those specific facilities. Certain types of communications are expressly forbidden. This includes the random mailing of messages; the sending of chain letters; mass mailings to all users of remote computer systems; the sending, forwarding, or intentional receiving of obscene, harassing, or threatening material, or the use of facilities for commercial purposes (Tier 2 infraction).
e. It is expressly forbidden to install any computer networks not endorsed by the state and by ASMSA. This includes, but is not limited to, running network lines from room to room (including going through the bathroom). Students may not run lines along the floor, attach lines to walls or ceilings by any means, or run lines through electrical conduits or heating/air ducts. Requests for exception to this policy must be submitted to the Network Administrator.

9. Web Pages/Internet
a. The school's computer system may be used to create, revise, and house home pages for the school, departments, school organizations/clubs, and personal home pages for the students, faculty, staff, administration, and board members. No other home page can be housed on the school's system without specific permission from the Network Administrator (Tier 2 infraction).
b. ASMSA is not responsible for Internet content. ASMSA employs a filtering system to block access to material of an inappropriate nature.
c. Students who post, create, or build any web site linked to ASMSA without the school’s knowledge or express permission will be subject to investigation by the Network Administrator and possible disciplinary action. All such sites will be reviewed for purpose, nature and content.

10. Harassment
Students may not use the school's voice/data connections to harass anyone. This includes the use of insulting, sexist, racist, obscene, or suggestive e-mail (Tier 3 infraction).

11. Attacking the System
a. Students must not attempt to degrade or subvert in any way the performance of the school's computer

system (Tier 3 infraction.)
b. Deliberately crashing the system is expressly forbidden (Tier 3 infraction).
c. Attacking the system is punishable under state law.

12. Waste and Abuse
a. Students must avoid any activity around their workstation that may result in damage to the computer, printer, software, or information. Eating and/or drinking is not allowed at any of the computer workstations (Tier 1 infraction).
b. The school's computer system should not be abused or wasted. Students should be considerate of fellow users, and avoid monopolizing computer systems and connect time, disk space, and other computer resources (Tier 1 infraction).
c. Network printers are placed at various locations for educational use. These printers should be used responsibly to prevent waste and abuse (Tier 1 infraction).

13. Hardware
a. No ASMSA computer hardware, peripherals, or cables may be moved or removed from their current location without specific authorization by the Network Administrator (Tier 2 infraction).
b. No student will attempt to service any ASMSA hardware without written authorization from the Network Administrator (Tier 2 infraction).

14. Workplace Monitoring
ASMSA has the obligation to ensure that its computer resources are used properly and within the established guidelines. ASMSA reserves the right to monitor the system for signs of illegal or unauthorized activity.

15. Enforcement
ASMSA will investigate any alleged abuses of its computer resources. As part of that investigation, ASMSA may access the electronic files of its users. If the investigation indicates that computer privileges have been violated, the Network Administrator or his/her designee may limit the access of users found to be improperly using computer systems. ASMSA may refer flagrant abuses to law enforcement authorities. Although ASMSA wishes to ensure that the privacy of all users of the network is protected, in the course of its investigation, ASMSA may reveal private, user related information to other employees or concerned parties. Any violation of ASMSA computer policy may result in a loss of some or all computer privileges. Act 801 of 1997 states that “students who use any technology in an inappropriate manner and/or not as directed by the school are in violation of school policy and subject to disciplinary action up to and including the loss of the right to use the technology (which may involve loss of credit if the technology use was for course work).” Legal action and/or dismissal from ASMSA may result from violations of state or federal laws. a. The Dean of Academic Affairs will hear all cases of student misuse of ASMSA computers.
b. Students may temporarily be denied access pending the Dean's review if there is a reasonable suspicion that the student may use his/her access to cause harm or do damage in the interim.
c. Penalties for computer infractions are as follows:
1) First offense Tiers 1 and 2 (non-malicious): warning.
2) Subsequent offenses Tiers 1 and 2: 5 class day suspension of one or more network privileges.
3) Tier 3: Ten class day suspension of one or more network privileges and probation.
d. A violation of the Computer Use Policy may also constitute a violation of the ASMSA Disciplinary Code. In this scenario there may be consequences issued by both the Dean of Academic Affairs and the Dean of Residential Affairs.