Villa Maria Academy Computer Network and Internet Acceptable Use Policy

Villa Maria aims to promote an open computing environment that allows technology access for all individuals. In order to protect its information assets, the school relies heavily on its computerized information systems and recognizes that all resources, including software programs, data, hardware, and networks, must be protected from misuse and operated and maintained in a secure environment. The use of computers and Internet access is a privilege and not a right. The school requires all students, parents/guardians, and teachers to sign a binding agreement, which acknowledges that they read the terms and conditions of acceptable use and understand their inherent responsibilities.

Electronic communications facilities available to members of VMA's students and faculty/staff are:

- Wireless network with Internet access
- G-Suite, Office, Adobe, Filtering, Curricular applications
- Application servers (such as Schoology, Turnitin, SCOIR, and PowerSchool)
- Student computer labs
- School Website/Staff Intranet/social media filters
- Cell phone and classroom phones
- Printers and copiers

Those permitted access to school's network or Internet services are responsible for using it in an effective, ethical and lawful manner. School communications include email, official school social media outlets Schoology or School Messenger systems. Because the AUP is part of the various Student and Staff Handbooks, an individual's agreement to abide by the AUP is implicit in his/her joining the Villa Maria Academy community as an employee or as a student. In addition, the Academy reserves the right to notify local, state and/or federal officials when it suspects that individuals are using the Academy's systems in violation of local, state or Federal laws. Villa network account holders who provide account access to unauthorized users will result in a loss of network privilege.

It is expected that a VILLA Email is the vehicle for student-teacher communication and only VILLA issued Email account will be used as a way of communicating between student and teacher.

EMAIL GUIDELINES:

1. **It is required of all users to check their Villa Email daily** for school announcements, academic information and general mail. This mailbox is a privilege and should be maintained by the user to ensure the mailbox items do not prevent the sending or receiving of mail by the user.

2. **Sending or displaying offensive messages, discriminatory, obscene language or pictures is prohibited.** Harassing, insulting, or attacking others is prohibited. This includes emails sent from the user's in-school account or another Internet or web account. Messages sent under an assumed name or modified address or with the intent to obscure the origin of the message is prohibited.

3. **Email is not guaranteed to be private.** The contents of these files and the copies on system backups, archived storage and g-suite are subject to investigation by the Director of Technology if suspicion of a violation occurs. All users must recognize that e-mail messages and other information transferred by the network may contain thoughts, conclusions and biased perceptions that were never intended for publication. There may be liability for defamation for spreading false and disparaging information about third parties, particularly comments on students, personnel applicants, or venders. Such discussions or use of the network is expressly prohibited.

4. **No one may distribute unwanted mail or other messages.** These includes, but are not limited to: chain letters, blogging, photos, mass mailing of jokes or lost and found items, and/or virus alerts.

5. **Additional technological activities:**

- No student or faculty/staff member shall use technology or school resources to engage in fake accounts on the Internet or on campus. Violations will be subject to disciplinary action. This is to hold true whether the use occurs on or off campus and whether using Villa Maria or personally owned devices. It is expected that all Villa Marians conduct their behavior appropriately and within the parameters of the Integrity agreement they sign.

- It is prohibited to retain a photo/video of a staff member to be used without his/her knowledge and consent on any social media or devices.

NETWORK GUIDELINES

1. Network users may not allow another person to log onto or otherwise access his/her accounts.

2. PASSWORD POLICY: Passwords must adhere to the 8-character policy adopted for use with Google Suite. If a student feels that her account has been tampered with, she should change her password immediately on all devices. It is suggested that passwords be changed every 90 days. Two-step authentication is also available on network accounts and can be turned on for users in settings.

3. If there is a problem with a Villa network account, profile settings, or Villa mail, it is the user's responsibility to report this to the network administrator.

4. The use of school computers is limited to educational purposes.

5. Users should keep only active files on their P Drive. All users are issued a personal drive on which to store projects and student work; these must be kept cleaned of old files and be content appropriate. Personal drives (P) sync files with Google drive so remote access to files is available from home. All student P drives will be deleted the week after graduation.

6. Users must strive to keep accounts and personal devices brought to campus free of viruses. All users should make sure that any personal computer brought to campus is protected from virus-related materials with appropriate software. Any computer flagged as corrupt will be refused access to the school network.

7. There is NO Food or Drink permitted in the lab areas or near any computer at any time.

8. Computer labs are to be maintained as quiet study areas. If a student wishes to listen to a school-related academic video on a school computer, headsets must be worn.

9. Cyberbullying is prohibited. Cyberbullying is the "willful and repeated harm inflicted through the medium of electronic media." It may involve sending mean, vulgar or threatening messages or images; posting sensitive, private or disparaging information about another person; pretending to be someone else in order to make that person look bad; or intentionally excluding someone from an online group. Reports of this behavior should be reported immediately to the administration or Director of Technology.

10. Students are responsible for their accounts and for all activity conducted with their accounts.

SCHOOLOGY (Academic Portal)

1. All Students, Staff and Parents will receive access to Schoology. Schoologyis VMA's academic portal where class information and extracurricular activity information is kept. All new students must activate their Schoology accounts at the start of their first academic year, and they will use their Villa email and password to access this resource. Students are encouraged to check Schoology daily for assignments, notes, and calendars. Additional library resources are available electronically for use off campus.
2. Cloud Storage is available for all users. All students have unlimited Google Drive space for storage of files.

POWERSCHOOL

1. Student Rosters, Grades, Emergency contacts/numbers and demographic information are posted on PowerSchool through the parent or student portal. Parents and students have individual access rights. Contact the PowerSchool Administrator for account help.

PERSONAL CONDUCT ONLINE

All Users are to be respectful of themselves and of the Villa Maria Academy name when posting to blog/social media sites off-campus. Students who carelessly post personal information about themselves that tarnishes their images or the image of the school should expected to be disciplined.

Villa Maria Academy reserves the right to impose consequences for inappropriate behavior that takes place off campus and outside school hours. Inappropriate use may include, but is not limited to:

● Harassment, use of school name, remarks directed to or about teachers, offensive communications and safety threats are prohibited
● Students are responsible and will be held accountable for what they post on public web sites.
● Students are prohibited from posing as faculty/staff online or creating accounts (Twitter, Facebook, etc.) using another person's identity or personal information. Anything inappropriate, not in line with the values and beliefs of VMA which is brought to the attention of the Dean of Students will result in disciplinary consequences including detention, suspension, and/or dismissal.

ADDITIONAL TECHNOLOGIES

1. There will be no cell phone use during the school day. Cell phones must be completely turned off and stored in book bags.
2. The teacher reserves the right to check the content of memory on student TI 83/84 calculators and free up memory space for academic purposes.
3. The School Administration reserves the right to limit or prohibit external devices in the classrooms such as personal laptops, PDA, calculators, wireless devices, etc. Any personal device of a student or staff member must have updated virus protection before use on the campus network.
4. Students are responsible to pick up all printed work from network printers during the school day. Please check the default printer before printing documents. If resources are abused, printing limits will be enforced.

COPYRIGHT/WEB USE GUIDELINES

1. It is inappropriate to invade the privacy of another by accessing, copying or distributing another's computer files or computer programs without consent.

2. A student or employee who inadvertently becomes part of a transfer of inappropriate material to or from the Internet is obligated to report the incident to the Network Administrator.

3. Copyrighted material must not be downloaded or used without the author's permission.

4. Vandalism of any kind will result in termination of computer privileges. Vandalism is any attempt to harm or damage computers, computer systems, or computer networks, or to infiltrate another computer system. These activities are prohibited, and the user is responsible for all repair costs incurred by the Academy as a result of such actions.

5. No student may use the VMA network for financial gain, hacking, creating or spreading viruses on the

School's network, selling or storing of non-academic materials on the servers or private drives.

6. A complete Copyright Policy is available on the Villa Maria Academy Schoology site. Any user who does not choose to comply with these guidelines will lose computer privileges for a period of time determined by the administration. Repeated infractions may result in permanent termination of computer and/or Internet privileges. Standard disciplinary procedures of Villa Maria Academy will apply.

iPADs and OTHER ELECTRONIC DEVICES:

1. All students are required to bring a fully charged iPad to school daily. Users will be allowed to connect to the VMA Wi-Fi Network for Internet access only. Filtered Internet access will be available for users with authenticated Wi-Fi personal devices.

2. Teachers have a right to manage and/or restrict student use of the iPad, laptops, software, and Internet within the confines of their class. Teachers will provide their acceptable use guidelines within their class materials. Students must secure the permission from each teacher in whose classes they plan to use their laptop.

The student must remain on task in that class while using it and any unauthorized use during class time such as email checks, web surfing, etc. will result in loss of use privileges.

3. Any unauthorized filming or photographing of any person or class is prohibited.

4. Charging Batteries: iPads and mobile devices should be brought to school each day in a fully charged condition. No classroom electrical provisions are available for devices that lose battery power during the academic day.

5. Sound. Sound should be muted at all times unless permission is obtained from the teacher for instructional purposes. If teachers require headphones it is student's responsibility to obtain and store them.

6. Identification and Use. All personal devices should be identifiable with student name on the device. A device should be securely stored when not in use and is the responsibility of the owner. All activity that is authored on the device is the responsibility of the registered owner of the device. All technical support is the responsibility of the owner.

NETWORK BACKUP and EMAIL RETENTION POLICY:

1. All network files (P and all network shares) are backed up Monday-Friday. Students should also plan to keep important files backed up to Google drive for personal archiving.

2. Email is archived through Google Vault daily for all users.

6/1/2019