Acceptable Use Policy ("AUP")

STUDENT NAME: _____ DATE: _____

Conchita Espinosa Academy ("School") is committed to student use of technology as a tool to expand learning opportunities and conduct scholarly research. The use of technology facilitates global collaboration--a vital skill for our 21st century learners. Students at the School utilize electronic devices on a wireless network. Electronic devices and the wireless network on the School's campus are strictly for educational use consistent with the School's educational goals. The use of the electronic devices on the School's campus is a privilege, not a right. Along with the opportunity this provides, comes responsibility. This Acceptable Use Policy is designed to give the student and the student's family, as well as others on the School's campus, clear and concise guidelines regarding the appropriate use of electronic devices. The underlying premise of this policy is that all members of the School community must uphold the values of honesty and integrity. We expect our students to exercise good judgment and to utilize technology with integrity.

E-Mail

- Students are only authorized to use their school email. Students may not access any other email service while at school unless authorized by or administration.
- Students must use appropriate language in their e-mail messages.
- E-mail services provided by the school are to be used only for the exchange of appropriate information.
- Inappropriate e-mail will not be tolerated, including derogatory, obscene, or harassing messages. E-mail messages of an abusive or harassing nature will be regarded as a major violation and will be subject to a disciplinary response, which may result in expulsion.
- Chain and mass e-mails and letters of any kind and spam are prohibited. Chain letters are defined as any email message asking you to pass information or messages to other individuals or groups via e-mail.
- E-mail etiquette should be observed. In general, only messages that one would communicate to the recipient in person should be written.
- School e-mail addresses are not to be given to ANY websites, companies, or other third parties without the explicit permission of a teacher or administrator.
- Only school-related attachments may be sent on the school e-mail system.
- The School e-mail is not intended for private use, and there is no expectation of privacy within the communications received or exchanged through it. The administration reserves the right to review any and all communication within it.

Chatting and Blogging

- Instant messaging is prohibited on campus.
- Blogging is to be utilized on campus, only for academic purposes.
- Participation in chat rooms during school hours is prohibited during the school day, except as part of an assigned, in-class activity.

Audio and Video

- The use of electronic devices to watch movies and videos, unless assigned by a teacher, is not permitted during the school day.
- Audio should be turned off or on silent unless required for the activity being conducted.
- Listening to music either on speaker or with earphones is not permitted on campus unless required for the activity being conducted.
- When sound is needed, headphones provided by the student must be used.
- Any audio or video recording may be done only with the prior permission of all parties being recorded.
- Streaming music over the school network is strictly prohibited and is subject to disciplinary action.

Games

- The viewing and/or playing of electronic games is not permitted during school hours, except as part of an assigned, in-class activity or as directed by faculty or administration.
- The school reserves the right to remove any game from a school electronic device that is considered inappropriate or impedes the educational purpose of the electronic device program.
- No games that are played over the school network are allowed.

Electronic Devices

- If cell phones, iPods and all other personally owned electronic devices are in school, they are to be turned off and securely stored at all times. These devices cannot be used while on campus, unless approved by the director or principal. The school is not responsible for loss or damage to these devices.
- Electronic devices must be in a student's possession or secured in a locked classroom or locker at all times. Under no circumstances should electronic devices be left in unsupervised areas, including school grounds, lunchroom, labs, on top of lockers, in library, unlocked classrooms, hallways, etc.
- If an electronic device is found to be unattended, it will be turned in to the principal's office.
- Do not consume food or beverages near the electronic devices.
- Do not lend your electronic device to other students.
- Do not borrow an electronic device from another student.
- Electronic devices must be carried and transported appropriately on campus. Failure to do so could damage the device.
- Electronic devices should be handled with care. Inappropriate treatment of school electronic devices is not acceptable.
- Students are entirely responsible for backing up their own data. Lost or damaged data is not the school's responsibility.
- No writing or stickers will be allowed on the electronic device and electronic device cases, and these are not to be defaced in any way.
- Students are not allowed to create any administrative passwords on their electronic devices.
- Students who are assigned iPads are expected to come to school with a fully charged battery on a daily basis.
- Students will not synchronize the electronic devices or add apps to their assigned electronic devices to include home synching accounts.
- Students may be required to check in their electronic devices for periodic updates and synching and will do so at school's request.
- Students are strictly prohibited from any action that violates existing AUP or public law

- Students are strictly prohibited from sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit material.
- Students are strictly prohibited from changing of the electronic device settings (exceptions include personal settings such as font size, brightness, etc.)
- Students are strictly prohibited from gaining access to other student's accounts, files, and/or data.
- Students are strictly prohibited from using of the School's internet for financial or commercial gain or for any illegal activity.
- Students are strictly prohibited from using of anonymous and/or false communications using messenger services (Ex. – MSN Messenger, Yahoo Messenger, etc.)
- Students are not allowed to give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, Ebay, email, etc.
- Students are strictly prohibited from participating in credit card fraud, electronic forgery or other forms of illegal behavior.
- Students are strictly prohibited from vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of School equipment.
- Students are strictly prohibited from transmitting or accessing or storing materials that are obscene, threatening or otherwise intended to harass or demean recipients.
- Students are strictly prohibited from bypassing the School's web filter or firewall.
- Students are strictly prohibited from using the electronic device to imply school's endorsement, including the support or opposition of the school with regards to any religious or political activity or issue.

A student who has knowledge (or reasonable suspicion) of a violation of the AUP must report the violation or suspected violation to the Technology Curriculum Director.

Network Access

- Students must not make any attempt to access servers or network information that is not available to the public.
- The utilization of proxy avoidance IP numbers and programs is strictly prohibited.
- Students may not use the school network for personal or private business reasons including but not limited to online ordering and purchases.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal law (Florida Computers Crime Act, Chapter 815, Florida Statutes). This includes tampering with hardware or software, vandalizing data, invoking viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.
- The School is not responsible for damaged or lost data transferred through our network or stored on electronic devices or our file servers.
- The School shall at any time limit the access to its network when there is a violation (or there is reason to believe there has been a violation) of school AUP policies, contractual agreements, state, federal laws or applicable regulations.

File Sharing

- File sharing is the public or private sharing of electronic data or space. Any program that creates a point-to-point connection between two or more computing devices for the purpose of sharing data is considered file sharing.
- File sharing of any kind is prohibited both on campus and off campus. The only exception to this is when it is a specific assignment given by a faculty member.

- There is a $50 re-imaging charge to remove any unapproved software or files.

Deleting Files

- Do not delete any folders or files that you did not create or that you do not recognize.
- Deletion of certain files will result in electronic failure and will interfere with your ability to complete class work and may affect your grades.
- There is a $50 re-imaging charge to correct system files.

Downloading and Loading of Software

- Students are not permitted to install custom/individual applications that require administrator privileges.
- The downloading of apps, music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
- Copyrighted movies may not be "ripped" from DVDs and placed on the electronic devices nor may copyrighted movies be downloaded to the electronic devices from the Internet.
- There is a $50 re-imaging charge to remove any unapproved software or files.

Internet Use

- The Internet is a rich and valuable source of information for education. Inappropriate materials are available on the Internet and are strictly prohibited.
- Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Plagiarism includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.
- If a student accidentally accesses a website that contains obscene, inappropriate or otherwise offensive material, he/she is to notify a teacher, the Principal, or the Technology Curriculum Director as quickly as possible so that such sites can be blocked from further access. <u>This is not merely a request; it is a responsibility</u>.

Privacy, Use, and Safety

- Students may not give any personal information regarding themselves or others through e-mail or the Internet including name, phone number, address, passwords, etc.
- Students are not to provide the e-mail address or other personal information regarding other students, faculty, or administration to anyone outside of the school without their permission.
- Students must secure and maintain private passwords for network and electronic device access. This is important in order to protect the privacy of each student. Do NOT share personal passwords or usernames.
- The school may in its discretion monitor electronic device activities, including logging website access, newsgroup access, bandwidth, and network use.
- Students are prohibited from accessing faculty, administration, and staffs file servers for any reason without explicit permission from the user or administrator of that electronic device.
- Students are prohibited from utilizing the command prompt interface. In addition to this, students are prohibited from using any method to obtain control of another person's electronic device through the use of their own electronic device.
- Students are prohibited from utilizing peer-to-peer networking or any method of file sharing unless authorized by the technology staff.

- No identifiable photographs of students, faculty, or administration will be allowed to be published on the Internet or used in print without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.
- Cyber-bullying is the use of electronic information and communication devices to willfully harm a person or persons through any electronic medium, such as text, audio, photos, or videos. Examples of this behavior include, but are not limited to:
    - Sending/posting false, cruel, hurtful or vicious messages/comments;
    - Creating or contributing to web sites that have stories, cartoons, pictures, and jokes ridiculing others;
    - Breaking into an e-mail accounts and sending vicious or embarrassing materials to others;
    - Engaging someone in electronic communication, tricking that person into revealing sensitive personal information and forwarding that information to others;
    - Posting of a student picture without their permission.

- Any electronic communication that creates a hostile, disruptive environment on the school campus is a violation of the student's and of the staff member's right to be safe and secure. Actions deliberately threatening, harassing or intimidating an individual or group of individuals; placing an individual in reasonable fear of harm; damaging an individual's property; or disrupting the orderly operation of the school will not be tolerated.
- Electronic devices that are provided by the school continue to be the property of the school. Therefore, the school has the right to view all content at any time.
- Any electronic device used on the school network, even if privately owned, is subject to all policies and consequences of the AUP including: the right to view the content of the device at any time; the right to remove content from the device; and the right to retain the device in the school's possession if there is an infraction to the AUP that deserves that consequence, as determined by the School's administration.

Copyright

- Unauthorized duplication, installation, alteration, or destruction of data programs, hardware, or software is prohibited.
- Data, programs, hardware, software, and other materials including those protected by copyright may not be transmitted or duplicated.

Consequences

- The school reserves the right to enforce appropriate consequences for the violation of any section of the AUP. Such consequences could include the loss of the privilege to use an electronic device, the loss of the use of the electronic device for an amount of time determined by the administration and Technology Curriculum Director, fines, disciplinary action (including expulsion from the school) and possible legal action.
- These consequences apply to students participating in the electronic device program at the School as well as to students who are using the school's electronic device off campus.
- Any electronic device with illegal or inappropriate software or materials on it will be reformatted or "re-imaged," and the student will be charged a $25 AUP violation fee PER incident for this service. This amount may be increased for repeat violations.
- In the case of repeated electronic device abuse and/or damages, the school has the right to revoke the use of the school's electronic device and the student will be restricted to using it only on-campus. Repeated AUP offenses or electronic device abuses may lead to the loss of a student's privilege of using an electronic device on campus.

- Students are to report any known violations of this AUP to appropriate administrative staff members. Random checks of student electronic devices will be conducted throughout the year to ensure that these policies are being followed.
- The School takes no responsibility for activities conducted on the electronic devices or materials stored on the electronic devices, or the school's network.

Student's Name _____

Student's Signature _____

Parent's Name _____

Parent's Signature _____