

Mother of Our Redeemer Catholic School iPads/ Computers Acceptable Use Policy 2017-2018

Student LN, FN:
Email:

Grade:

Date:

Mother of Our Redeemer Catholic 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 Apple iPad on a wireless network. Apple iPads and the wireless network on the School's campus are strictly for educational use consistent with the School's educational goals. 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 Apple iPads. The underlying premise of this policy is that all members of the School's 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

- The School has provided a filtered and monitored Office 365 student email.
- Proper use of e-mail must be consistent with the Acceptable Use Policy and iPad Use Agreement.
- It must be used strictly for educational purposes, and as directed and approved by faculty or administration.
- E-mails to recipients outside of the Mother of Our Redeemer domain is strictly forbidden, except as part of an assigned, in class activity that is supervised by faculty or administration.
- No personal Emails are to be added to the iPad and they will not be allowed on campus network

OneDrive

- The School has provided a OneDrive Cloud Drive .
- All files, notes, etc. created by student must be saved on the One Drive.
- Proper use of the Drive must be consistent with the Acceptable Use Policy and iPad Use Agreement.
- It must be used strictly for storing and accessing school-related files.
- No music, movies, videos, pictures, games or any media files are to be stored, except as part of an assigned activity by faculty or administration.

Chatting and Blogging

- **Instant messaging is prohibited on campus except as part of an assigned, in class activity that is supervised by faculty or administration.**
- **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

- Audio on the Apple iPads should be turned off unless required for the activity being conducted.
- Listening to music either aloud or with earphones is not permitted on campus unless required for the activity being conducted. Faculty and staff may relax this policy at their discretion.
- When sound is needed, headphones provided by the student must be used.

- **The use of Apple iPads to watch movies and videos, unless assigned by a teacher, is not permitted during the school day.**
- Any audio or video recording may be done only with the prior permission of all parties being recorded.
- **Sharing of music (including iTunes music sharing) 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.**
- The school reserves the right to remove any game from a student's iPad that is considered inappropriate or impedes the educational purpose of the Apple iPad program.
- No games that are played over the school network are allowed.
- Games that include violence, adult content, inappropriate language, and weapons are not to be installed or played on the Apple iPads.
- Screensavers that include gaming components are not allowed.

Apple iPads

- Student Apple iPads must not be left unattended at any time. If an Apple iPad is found to be unattended, it will be turned in to the School Office.
- Apple iPads must be in a student's possession or secured in a locked classroom at all times.
- Do not lend your Apple iPad to other students.
- Do not borrow an Apple iPad from another student.
- Apple iPads must be carried and transported appropriately on campus. They should be carried in their approved cases at all times. Failure to do so could damage the device and result in permanent loss of data.
- *Note:* Students are entirely responsible for backing up their own data. Lost or damaged data is not the school's responsibility. All Apple iPads must be in the iPads case.
- Do not consume food or beverages near the Apple iPads. Apple iPads may not be used in the Cafeteria during lunch.
- Apple iPads should be handled with care. Inappropriate treatment of Apple iPads is not acceptable.
- Students are not allowed to create any administrative passwords on their Apple iPads.
- Students are expected to come to school with a fully charged battery on a daily basis; however, should the Student's Apple iPad run out of battery, the Student can charge the iPad in their homeroom.
- Jailbreaking an Apple iPad is strictly prohibited. If an Apple iPad is jailbroken, the Student's parents will be responsible for restoring iPad and any technology fees. Associated with adding iPad back into the schools network.
- There is a \$25 re-imaging charge to restore iPad to original software.

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 Computer-Related Crimes Act, Chapter 815, Florida Statutes). This includes tampering with iPad hardware or software, vandalizing data, invoking iPad 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 Apple iPads or our file servers.

File Sharing

- File sharing is the public or private sharing of iPad 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.
- No file sharing software of any kind is to be installed on the Apple iPads. Examples of this type of software are Limewire, Bearshare, Kazaa, iMesh, etc. Although these types of programs are software downloads, they automatically create file sharing connections.
- There is a \$25 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 iPad failure and will interfere with your ability to complete class work and may affect your grades.
- There is a \$25 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.
- All installed software must be a legally licensed copy.
- The downloading of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
- The school reserves the right to remove any software that has been loaded onto the iPad that impedes the educational purpose of the Apple iPad program.
- Copyrighted movies may not be "ripped" from DVDs and placed on the Apple iPads nor may copyrighted movies be downloaded to the Apple iPads from the Internet.
- If administration approves, only commercial videos (such as television programs) legally purchased from the iTunes music store or another like entity may be downloaded to the Apple iPads.
- Shareware and freeware programs such as animated cursors (i.e. Comet Cursor), screen savers, and other programs similar to these, automatically open connections outside the School's network. Such connections are Spyware, and they not only monitor the activities on that iPad, but they also slow down the operation of the iPad and the network connection.
- There is a \$25 re-imaging charge to remove any unapproved software or files.

Screensavers

- Inappropriate or copyrighted media may not be used as a screensaver.

- Pictures or videos which include the presence of weapons, pornographic materials, inappropriate language, alcohol, drug, gang-related symbols or pictures will result in disciplinary actions.
- There is a \$25 re-imaging charge to remove any of the above

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. These materials include items of a sexual or pornographic nature, extremist or militant materials, gambling, depictions of violence, images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.
- Information obtained through the Internet must be properly cited and in compliance with copyright laws. Due to the quickly changing nature of the Internet, a hard copy of referenced material is recommended.
- 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, pornographic or otherwise offensive material, he/she is to notify a teacher, the Network Administrator, or the Technology Coordinator as quickly as possible so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

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. unless they are completely sure of the identity of the person with whom they are communicating. Frequently the identity of someone on the Internet is impossible to confirm. Therefore, contact with such individuals is considered inappropriate and unsafe.
- 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 Apple iPad access. This is important in order to protect the privacy of each student. Do NOT share personal passwords or usernames.
- The School respects the privacy of every student, faculty member, and administrator with respect to stored files and e-mail accounts. However, if inappropriate use of e-mail accounts or the School's network, including honor code violations or harassment, is suspected, the school's administration has the right to view these files in order to investigate suspected inappropriate behavior.
- The school will monitor iPad activities, including logging website access, newsgroup access, bandwidth, and network use.
- Students are prohibited from accessing faculty, administration, and staff's file servers for any reason without explicit permission from the user or administrator of that iPad.
- 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 iPad through the use of their own iPad.
- 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 websites that have stories, cartoons, pictures, and jokes ridiculing others;
 - Breaking into an e-mail account 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.
- Apple iPads 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 iPad, the loss of the use of the iPad for an amount of time determined by the administration and members of the Technology Department, possible disciplinary action and possible legal action.
- These consequences apply to all students using iPads on campus.
- Any iPad 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.
- Repeated AUP offenses or Apple iPad abuses may lead to the loss of a student's privilege of using an Apple iPad on campus.
- Students are to report any known violations of this AUP to appropriate administrative staff members. Random checks of student Apple iPads will be conducted throughout the year to ensure that these policies are being followed.

- The School takes no responsibility for activities conducted on the Apple iPads or materials stored on the Apple iPads, or the school's network.

Florida Computer-Related Crimes Act

Fla. Stat. 815.04 Offenses against Intellectual Property

Whoever willfully, knowingly, and without authorization,

1. modifies data, programs, or supporting documentation residing or existing internal or external to an iPad, iPad system, or iPad network;
2. destroys data, programs, or supporting documentation residing or existing internal or external to a iPad, iPad system, or iPad network; or
3. discloses or takes data, programs, or supporting documentation which is a trade secret as defined in S.812.081 or is confidential as provided by law residing or existing internal or external to a iPad, iPad system, or iPad network;

Commits an offense against intellectual property and is guilty of a felony in the third degree punishable by up to 5 years' imprisonment and a fine of up to \$5,000.

Fla. Stat. 815.06 Offenses against iPad Users

Whoever willfully, knowingly, and without authorization,

1. accesses or causes any iPad, iPad system, or iPad network to be accessed; or
2. denies or causes the denial of iPad system services to an authorized user of such iPad system services;

Commits an offense against iPad users and is guilty of a felony in the third degree punishable by up to 5 years' imprisonment and a fine of up to \$5,000.

If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree punishable by up to 15 years imprisonment and a fine of up to \$10,000.

Apple ID:

Student ID #:

Student Name

ID Number

Student Signature

Date

Parent (Guardian) Name

Parent (Guardian) Signature

Date