NOTRE DAME
PREPARATORY SCHOOL AND MARIST ACADEMY

TECHNOLOGY RESPONSIBLE USE POLICY

The Technology Responsible Use Policy is provided so that students and parents are aware of the responsibilities students accept when they use school-owned computer, hardware, peripherals, operating system, application software, eBooks, data files, school email, digitized information, online resources, communication technologies, and Internet/network access. In general, this requires efficient, ethical, legal and mission oriented utilization of all technology resources.

Notre Dame Preparatory School and Marist Academy (NDPMA) is entrusted to offer our students the latest developments in valuable educational technologies. With the privilege as a student to use the technologies and resources, comes the responsibility to use them correctly.

Families and students agreed to have read and understood said policy on the registration form. All users are expected to comply and use technology at NDPMA in a constructive and educational manner.

RESPONSIBLE USE
Technology resources are provided to all students for educational purposes. Each student should be aware of the following items to maintain their technology privileges at Notre Dame Preparatory and Marist Academy. Noncompliance may result in restrictions of technology privileges and possible disciplinary actions.

- Students are responsible for their ethical and educational use of the computer and their internet connection whether accessing the network from outside the school.

- Students are fully responsible for the security of all devices and accessories from theft, loss, or damage.

- Preserve the integrity of the computer systems by only downloading approved software and uploading appropriate files as approved by a teacher, school administrator, or the IT Department.

- Maintain the privacy of all users by accessing only your own accounts, files, and school email. Login only with your own NDPMA username and password.

- Respect all user passwords. Protect another student's files and privacy as you would want your privacy protected. Should you come across or gain knowledge of a password that is not yours, tell the person right away to change their password.

- Address all inappropriate pictures, images, or emails quickly and quietly with a teacher, administrator, or librarian. Attract very little attention from your surroundings and never share an inappropriate picture, image, or email with another student.

- Follow closely all guidelines established by a teacher who utilizes a Social Media/Networking site for the classroom sharing of information. Responsible use extends to all off-campus activities.

- Print only when necessary. Printing supplies are costly but more importantly it has a negative impact on our precious environmental resources.

Last updated: July 18, 2017

- Explore the Internet as a powerful research tool with a critical eye for the legitimacy of the resource. Determine the quality of all sources before including it in your research and properly cite all materials included in your research.

- Be polite, use respectful and appropriate language at all times in all communications. Bullying by any means will not be tolerated. Every communication creates a digital footprint that will represent you today, tomorrow, and for many years in the future.

- Avoid revealing personal and/or confidential information online, be aware of phishing scams.

- Although the school has Internet filtering in place, it is still possible for students to encounter inappropriate material. Students are expected to notify a faculty/staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

- Avoid transmitting any material which is in violation of any federal or state law.

- Students who identify or learn about a security problem are expected to convey the details to their teacher or other school staff without discussing it with other students.

- Students may not use a faculty/staff computer without permission from said faculty/staff member.

- Responsibility to keep computer devices secure lies with the individual student. NDPMA is not liable for any device stolen, infected, or damaged on or off campus including school functions.

- Do not use the schools branding without permission nor create spoof NDPMA social media accounts.

- Use chat tools\applications such as Skype and Google Hangouts for educational purposes.

- Students are to use their school issued device to connect and use each day for educational purposes.

- Students should follow teacher instructions regarding technology use in their respective classrooms.

- Students should access their school email accounts at least once day for any important communication from the school and/or teachers.

- Students should use their school email accounts and avoid using personal email accounts for school related communication. E-mail should be used for educational or administrative purposes only. Avoid spamming.

- Avoid allowing technology to disrupt the classroom, learning process, or other school functions. Be mindful of speaker levels, distractive screen displays, and other noise that may cause a classroom distraction.

- Be mindful to not waste limited school internet resources by causing congestion on the school network through online video gaming, or streaming music and/or videos.

- Avoid circumventing NDPMA Internet filtering system by modifying the network settings on your school issued device by using unauthorized software/tools or mobile data.

- School owned devices should not be serviced by anyone outside of the school, bring the device to IT for all technical support, maintenance, malfunctions, or warranty claims. This includes self-repairs by students.

- Technology should be used to assist students in their learning. Cheating using a computer device, communication network, or any other technology is not tolerated by the school.

NETWORK USAGE

Access to the NDPMA network is a privilege and not a right. Each student, and/or parent will be required to sign the Technology Responsible Use of Policy in order to be granted access to the secured school network.

- NDPMA network is for school related activities only. Utilizing the network or resources for financial gain, to break copyright laws, or for any commercial or illegal activity is strictly forbidden.

- Students should not attempt to bypass the NDPMA filtering or firewall system in anyway.

- The NDPMA network has been established for a limited educational purpose. The use of the network must be in support of education and research that supports NDPMA's educational goals and objectives.

- NDPMA reserves the right to monitor internet usage to ensure that its policies are being adhered to. Use of the school technology system constitutes consent to monitoring for these purposes.

- Personal data plans are not permitted during core school hours. Access to the NDPMA network is available to all students for school or personal devices. Secured access is provided by the IT department.

- All email communications are filtered for appropriate and academic use. Administrators may review communications to maintain system integrity and ensure that students are using the system responsibly.

- Electronic mail, network usage, computer use, and all stored files shall not be considered confidential and may be monitored at any time by designated school staff to ensure appropriate use.

- NDPMA may selectively limit bandwidth, filter, or block Internet applications and content as needed.

- To comply with Children's Internet Protection Act (CIPA) filtering and monitoring: NDPMA has deployed technology which attempts to filter abusive, defamatory, obscene, violent, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material.

- NDPMA IT Administrators shall make reasonable efforts to restrict access to inappropriate materials and shall monitor the online activities, as reasonably able, of the end users in the school environment. Therefore, will add or remove sites as necessary to comply with CIPA.

CYBERSECURITY AND PRIVACY

School issued devices are not private and may be examined by a school administrator to protect the security and safety of a student or our community.

- Users have the primary responsibility to protect the confidentiality of their system and passwords.

- Users associated to a system account or device will be responsible for its appropriate use at all times.

- Users should refrain from using school technology systems to convey any confidential or personal data.

- Users shall not access information for which the individual(s) do not have privilege.

- Users will not engage in knowingly placing malicious software or viruses on a computer or the network.

- Users should avoid violating copyright laws, plagiarism, or privacy of others.

- Users shall not bring their own personal device to use during school hours, nor will personal devices be supported by the IT department.

- User should not circumvent or disable protection measures installed or put in place by the IT Department.

CONSEQUENCES FOR MISUSE

The use of electronic information resources and the electronic device may be revoked or limited at any time. The school administration reserves the right to address any incidents involving the use of the electronic device on a case-by-case basis.

Administration has the right to issue disciplinary consequences based on but not limited to school policies. Possible consequences include, but are not limited to the following:

- Loss of use of the device completely or limited to use only during the regularly scheduled school day

- Reset the operating system of the device to wipe the system clean

- Removal of administrative rights from their device

- Reporting of the incident to parents and/or local law enforcement

- Some violations, because of misuse of the technology, may result in monetary fines

DIGITAL CITIZENSHIP:

In our changing digital world, it is very important to be always mindful of your online reputation and to take every precaution to safeguard it. This agreement is intended to help you develop the habits of good digital citizenship.

- I agree not to submit, publish, display, or retrieve any defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, cyber bullying/bullying, or illegal material.

- I understand that the use of any electronic communications to harass or bully another is unacceptable and will be addressed by the administration. If I am being bullied or harassed, I will report it to a trusted adult so that the behavior can be addressed.

- I understand that the use of electronic information resources must be in support of education, research, and the educational mission and core values of Notre Dame Preparatory and Marist Academy.

- I will abide by all copyright regulations and understand that copyright guidelines are available in the Media Center or on request from the librarians.

- I will accept personal responsibility in reporting any misuse of the network to the school administration.

- I will use information systems resources for educational purposes only.

- I will not use the school network in any way that disrupts the use of the network for others.

- I will not attempt to bypass network or filtering settings configured by the school.

- I will avoid starting or participating in any email chain or chat communication that is not mission oriented.

- I will protect my personal information from outside forces that may cause harm or misuse details.

Last updated: July 18, 2017