PROVIDENCE CATHOLIC HIGH SCHOOL
RESPONSIBLE USE POLICY

For the use of the Providence Catholic wired and wireless networks, internet access, computers, mobile devices, and Microsoft Office 365 and Internet applications

Definitions:

- **User** includes anyone, including employees, students and guests, using PCHS technology, including but not limited to computers, wired or wireless network, Internet, email, Edline, and other forms of technology services and products.
- **Network** is wired and wireless technology networks, cellular networks, commercial, community or home-based wireless networks accessible to students.
- **Equipment** refers to cellular phones, smartphone devices, mp3 players, desktop computers, mobile devices such as laptops, iPads, kindles, e-readers, tablets, laptops and notebooks as well as portable storage devices.

Technology provides students with unique and powerful ways to enhance their learning. Providence Catholic High School (PCHS) supports the use of technology for the purpose of enhancing and supporting learning and is pleased to offer students access to our local area network and school-supplied technology resources to enhance and support learning.

It is one of the technology goals of the school to ensure that each user's interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through both personal and PCHS-owned devices inside or outside of our school that degrades or defames other users, or members of the PCHS community is unacceptable. PCHS recognizes that students have widespread access to both technology and the Internet. Therefore, use of personal devices and connectivity is considered to be included in this Responsible Use Policy (RUP).

Use of the technology resources and devices must be in support of educational goals, particularly during the school day. Technology resources are provided for students to conduct research, complete assignments and communicate with others. Access is provided to students who agree to act in a safe and responsible manner. Students must comply with PCHS standards and the PCHS student conduct code. It is expected that the users act in a responsible manner, and will honor the terms and conditions set by the teachers and the school. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. Students will be held accountable for their actions and are encouraged to report any accidental misuse immediately to their teacher or other school personnel.

No Expectation of Privacy

Network storage areas are property of the school and will be treated as such. Users should have no expectations of privacy regarding their use of PCHS property, network, Internet access or files, including email and all school-provided accounts. School officials may review files and communications at any time to maintain system integrity and confirm that all users are acting responsibly. With the increased usage of free educational applications on the Internet, digital storage areas containing user information may or may not be located on our local servers. Users should not expect that files and electronic communication are private. PCHS reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communications or files and disclose them to others as it deems necessary. This applies to use of personal devices as well as school-owned equipment.

PCHS will utilize filtering software or other technologies to prevent users from accessing visual depictions that are obscene, pornographic or harmful to minors. Despite every effort for supervision and filtering, all users are advised that access to the Internet may include the potential for access to content inappropriate for students and the school setting.

Every user must take responsibility for his/her use of the network and make every effort to avoid such content. Every user must report security or network problems to a teacher, administrator or system administrator.

Attempts to circumvent the PCHS content filter are strictly prohibited and will be a considered a violation of this RUP. PCHS will monitor online activities of users through direct observation and other technological means.

Inappropriate Activity

PCHS reserves the right to take other immediate action regarding activities that create security and/or safety issues for the PCHS network, users, school, devices or by other means that expend PCHS resources on activities which are determined to lack legitimate educational content/purpose, or other activities as determined by PCHS as inappropriate.

Examples of inappropriate activity include, but are not limited to:

- Engaging in practices that threaten the security of the network and resources, or interferes with other users, the network and equipment. Examples of such use are hacking, spamming, online gaming, propagation of viruses, broadcast messages, and chain letters.
- Using the network for non-academic bandwidth intensive activities such as network games, or transmission of large audio/video files or serving as a host for such activities.
- Intentionally wasting limited network resources (e.g., printing supplies, network space, and bandwidth).
- Bypassing or attempting to circumvent network security, virus protection, network filtering or policies.
- Abusing, altering or attempting to alter the configuration of a workstation, network device, operating system or software application in any way.
- Downloading, installing or attempting to install unauthorized software applications.
- Using others' passwords, or sharing your own password; attempting to gain access to others' passwords, to modify others' passwords.
- Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.
- Deleting, copying, modifying or forging other users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.
- Participating in online discussion boards or blogs without teacher direction.
- Violating copyright laws.
- Transmitting personal information, such as complete name, address, phone number, identifiable photo, schedule, of activities, and other confidential data about one's self or anyone else.
- Intentionally accessing, publishing or transmitting material which may be dangerous, immoral, defamatory, illegal or libelous as well as any material which ridicules, embarrasses, harasses, or in any other way harms another person, particularly members of the PCHS community.
- Using profane, abusive or impolite language.
- Any form of gambling or any game of chance, including illegal lotteries, sweepstakes and contests.
- Employing the network for commercial purposes, political purposes, financial gain, or fraud.
- Selling or purchasing illegal items or substances.

Violations may result in a loss of access to PCHS technology resources as well as other disciplinary or legal action as listed in the PCHS Student-Parent handbook, and as determined by school officials.

Microsoft Office 365 in Educational Applications

PCHS provides users with an educational suite of web applications for use to enhance teaching and learning. Microsoft Office 365 uses "cloud computing" where services and storage are provided over the internet. Systems Administrators have the capability to limit messages based on where they are from, where they are going, or the content they contain. PCHS will use these protection measures to block or filter, to the extent practical, access of visual depictions that are obscene, pornographic and harmful to minors over the network.

For users to gain access to his/her Microsoft Office 365 account, parental permission must be granted for a minor under the age of 18 years. Users 18 years of age or older are also required to acknowledge and accept PCHS's terms and conditions prior to obtaining access to technology within our school. All users, no matter the age, can accomplish this by signing the school RUP form.

Interactive Web Tools and Online Activity

Technology provides and abundance of opportunities for users to utilize interactive tools and sites on public websites that benefit learning, communication, collaboration and social interaction.

Users will be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school. During the course of the school year, teachers may recommend and use public interactive sites that, to the best of their knowledge, are legitimate and safe. As the site is "public" and the teacher and PCHS are not in control of it, all users must use their discretion when accessing information, storing and displaying work on the site.

Online communication is critical to the students' preparation for college and life beyond high school. Tools such as blogging, online discussion boards, podcasting, etc. offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers and students themselves.

Therefore, all users of online sites and service such as Microsoft Office365, PlusPortal, classroom discussion boards, student email, podcast projects, SharePoint sites, and other Web interactive tools should abide by all established safety and responsible use guidelines including:

- The use of Microsoft Office365, PlusPortal, classroom discussion boards, podcasts, SharePoint sites and any other web tool as directed by the teacher is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in the online setting.
- Students using such tools agree not to share their username or password with anyone except their parents or teachers. They agree to treat web posting space as a classroom space.
- Students should never post a link to a website without ensuring sure it is appropriate for the school setting.
- Students using Microsoft Office365 OneDrive, PlusPortal, discussion boards, podcasts, SharePoint sites or ANY other web tools are expected to act safely by keeping <u>all</u> personal information out of any post or communication.
- Students should NEVER, under any circumstance, agree to meet someone they have met over the Internet.
- Students should have no expectation of privacy when publishing or communicating online. ANY published data can be viewed and may be saved by others who have internet access.

Student Use of Mobile Devices and Personal Devices

Students are required to have a mobile device in compliance with our BYOD policy. Students must have a device that meets the minimum specifications as stated in our BYOD policy. Cellular phones do <u>not</u> meet the minimum specifications. Furthermore, cellular phone use is NOT allowed during the school day.

PCHS may provide some students with a device for use both in school and off-campus. The use of these PCHS-owned devices must follow the stipulations outlined in this RUP as well as any additional agreements specific to that device. Violations will result in disciplinary or legal action as determined by school officials.

Students may use personal electronic devices in the school setting only with the permission of the classroom teacher or other faculty member. The faculty member reserves the right to forbid any personal electronic device use during class or individual appointment at any time.

The use of a personal electronic device at school must be related to instruction or sanctioned school activities. The use of any personal device on school property must conform to all aspects of this RUP. When brought on school property, these devices are subject to search and may be confiscated pending review of appropriate disciplinary action.

No unauthorized wireless device will be attached to the PCHS private or public network without expressed permission. Doing so will be considered a network security breech and dealt with accordingly.

Students may not photograph, record audio, video or other digital media unless they have permission from both a faculty member and those whom they are recording.

School officials may search the student's personal or school-owned device if they feel school rules have been violated. This includes, but is not limited to, audio and video recording, photographs that violated others' privacy, or other issues regarding bullying, harassment, dangerous, immoral or defamatory content, etc.

All terms and conditions in this RUP apply to both school-owned and user-owned devices. Students using mobile and cellular devices while at school, during school or school-sponsored activities and events are subject to all terms and conditions in this document and are accountable for their use.

This document is subject to change without notice.
Last updated May 1, 2017