PASS CHRISTIAN PUBLIC SCHOOL DISTRICT
ACCEPTABLE USE POLICY

Revised 05-15

The Pass Christian School District is pleased to offer students and staff members access to the district's computer resources including the Internet. The use of technology is an integral part of the mission of the Pass Christian Public School District. The district also recognizes that mobile phones and digital devices are now an integral part of our student's culture and way of life and can have considerable value, particularly in relation to individual safety. Such technology will play a significant part in the education of the 21st century student, but, this use should follow agreed rules and guidelines to prevent classroom disruption, student misuse and teacher difficulties.

INTERNET POLICY AND GUIDELINES:

The Internet can provide a vast collection of educational resources for students and employees. Access to the Internet will enable students to explore thousands of libraries, databases, and sites containing educational information. Because information and services appear, disappear, and change constantly, it is not possible to predict or control what students may locate on any given day. Thus, the school district and associated employees make no guarantees pertaining to the accuracy of information received on the Internet. Although students will be under the supervision of their teachers and other staff members, it is not possible to constantly monitor individual students and what they may be accessing on the Internet.

Student's parents/guardians should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive. The Pass Christian School District is in compliance with the CIPA and COPPA. The district uses filtering to block offensive sites. While it is the school district's intent to make Internet access available to further educational goals and objectives, students may find ways to access other materials.

Students and staff are expected to follow all guidelines stated in this policy, as well as those directions and instructions given by members of the faculty, staff, or administration. Each student and staff member is required to demonstrate ethical behavior of the highest order when accessing computer resources. The privilege of using the district's computer resources requires proper and responsible use of the network, including the Internet.

Since access to the network is a privileged opportunity provided by the Pass Christian Public School District, any actions that might harm the computer equipment or software, impair their effective use, or show disregard for the procedures set up for network access will not be tolerated. The use of the network by students is subject to monitoring by teachers and/or administrators at all times and improper student conduct while accessing information on the network will be subject to disciplinary action.

1. Prior to use of the computer network, students must obtain parent/guardian signature on permission forms along with their own signature. These signed forms must be turned in to the designated school official.
2. Students and staff should never allow others to use their account numbers, access codes, or passwords, or attempt to use account numbers, access codes, or passwords not intended for personal use.
3. It is both a violation of law and this policy to access any network files, documents, applications, etc. that a user is not authorized to access.

4. The school shall inform parents that although internet access is filtered, their child may encounter information on the network, through the Internet, bulletin boards, or e-mail that is obscene or offensive. The student is responsible for not pursuing such material and shall be subject to disciplinary action if they engage in such activity. In addition to pornography, students must refrain from viewing or, utilizing in any way, any information that condones violence, hatred of others, or use of any weapon, substance, or material that may be hazardous to one's self or others.
5. The school shall educate minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, as well as cyber bullying awareness and response.
6. Electronic communication is not guaranteed to be private. The district reserves the right to monitor network, Internet activity and update filtering policy as deemed necessary.

7. Violation of any part of this policy shall result in strict disciplinary action, the extent of which will be based on the level of offense and determined at the discretion of a school or district administrator or their designee. Extreme violation of ethics, security, or safety standards may result in expulsion, dismissal, or legal prosecution.

Acceptable Use Policy guidelines for internet use include, but are not limited to the following:

1. Student use of the Internet must be curriculum related.
2. Students may not reveal personal information such as address, telephone number, or personal photographs over the Internet.
3. Students may not transmit credit card numbers, bank account information, or other financial information.
4. Students may not download executable, compressed, video, or music files.
5. Students may not participate in Internet Chat Rooms or social networking sites such as Twitter and FaceBook from school computers.
6. Students may not change any computer configurations including desktop backgrounds and screensavers.
7. Students must follow all other computer-use rules or procedures set forth by a teacher or administrator.
8. Use access time wisely. Do not tie up the network with idle activities.
9. The use of Proxy sites to circumvent filtering is prohibited.
10. Do not remove or damage any parts on the computer or its peripherals.
11. Do not attempt to access, change or delete files not intended for one's own use.
12. Do not play non-educational games on district computers.
13. Do not access Internet sites of questionable educational value.
14. Do not wastefully use computer supplies such as paper, printer cartridges, or disk space.
15. Use of district resources to transmit inappropriate language or potentially offensive material is prohibited.
16. Use of district resources to facilitate an illegal activity is prohibited.
17. Use of the district's computers for non-school related activities must be approved by the school principal.
18. School computer equipment or peripherals may not be moved to a different room or building without following proper fixed asset tracking procedures.
19. Falsely representing information found on the Internet as being your own is an act of plagiarism. Always give appropriate credit to original authors.
20. Anyone installing unauthorized software, or making unauthorized copies of copyrighted software assumes all legal responsibility for their actions and is subject to penalties imposed

upon by the district. Questions regarding software licensing should be directed to the District Technology Coordinator.

21. Internet postings on the district's web site must be approved by an appropriate administrator appointed by the District Technology Coordinator.
22. Do not connect personal devices (wired or wireless) to the district network without approval from the District Technology Coordinator.

Consequences of Internet Use Violations include but are not limited to:

1. Suspension of computer or network access
2. Revocation of computer or network access
3. School suspension
4. School Expulsion
5. Legal action and prosecution by proper authorities.
6. Any other consequence deemed necessary by the school principal or central office administrators.

MOBILE PHONES AND DIGITAL DEVICE POLICY AND GUIDELINES

Parents should be aware of and accept the potential disadvantages of mobile devices being allowed at school.

- Mobile devices may be damaged, lost or stolen.
- Students can be bullied by text messaging or other means.
- Mobile devices can be used to access, store and communicate inappropriate material.
- They can disrupt the learning environment.
- Students with mobile devices that have Internet access plans have the capability of accessing an unfiltered internet.
- Camera functions can lead to child protection and data protection issues with regard to inappropriate capture, use or distribution of images.
- In some instances data or usage fees on mobile devices may increase.

In an effort to prevent the disadvantages and to provide a safe learning environment for the student, the Pass Christian School District has developed and will enforce the following Acceptable Use Policy for Mobile Devices (AUPMD). Parents should read the policy and discuss it with their child prior to allowing them to bring a mobile device to school.

General Conditions for Mobile Device Use

1. The term mobile device in this policy denotes mobile phones, laptops, Ipod touches, tablets such as the Ipad or Android OS device or any similar mobile device that can access the Pass Christian School District's network.
2. Students, their parents or guardians must read and sign the Acceptable Use Policy for Mobile Devices before students are given permission to bring mobile devices to school.
3. Use of a mobile device must adhere to the District's AUPMD.
4. The AUPMD also applies to students during school excursions, camps and extra-curricular activities.
5. Parents are reminded that in cases of emergency, the campus office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.

6. File Storage on the network or Internet dropbox from personal mobile devices is limited to school work only. Anything not directly related to school work can be removed by the Technology Director or school official.

Responsibility of Students and Parents

1. It is the responsibility of students who bring mobile devices to school to abide by the guidelines outlined in this document. Failure to follow these guidelines may subject the student to the District's Code of Conduct or loss of use of the device.
2. The decision to provide a mobile device to their children should be made by parents or guardians and they should be aware if their child takes a device to school.
3. Permission to have a mobile device at school while under the school's supervision is contingent on parent/guardian permission in the form of a signed copy of this policy. Parents/guardians may revoke approval at any time.
4. In case of illness, students should follow the proper campus procedure for contacting parents and checking out of school through the office. Failure to do so may result in the action being subjected to the Student Code of Conduct.
5. In the event a mobile device is brought to school without a signed agreement by the parent, the student by the fact of bringing the device onto a campus implies agreement to accept the rules governing mobile devices.
6. Responsibility for the mobile device rests with the student and the District accepts no financial responsibility for damage, loss or theft. The student should keep the mobile device secure and locked away in their locker/bag when not in use. They should not leave it in any open area unattended.
7. All costs for data plans and fees associated with mobile devices are the responsibility of the student.

Acceptable Use of Mobile Devices

1. Specific acceptable use of a mobile device will be determined by each campus. These policies will be stated in the campus' Student Handbook.
2. Each teacher has the right to allow or disallow the use of mobile devices that support student achievement during instructional time as appropriate. Each teacher has the right to determine whether mobile devices must be stored out of sight or placed on the student's desk in plain sight when not used for instructional purposes.
3. Mobile devices with Internet access capabilities will access the Internet only through the school's filtered network while on school property during school hours.
4. Mobile devices should not be used in any manner or place that is disruptive to the normal routine of the class/school.
5. While on school premises during school hours, cell phones should be turned off when not in use.

Unacceptable Use of Mobile Devices

1. Any use of a mobile device that interferes with or disrupts the normal procedures of the school or classroom is prohibited. This prohibition extends to activities that occur off school property and outside of school hours if the result of that activity causes a substantial disruption to the educational environment.
2. Unless express permission is granted, mobile phones should not be used to make calls, send text messages, surf the Internet, take photos or use any other application during school lessons and other educational activities, such as assemblies.
3. Using mobile phones or devices to bully and threaten other students is unacceptable and will not be tolerated.

4. Pictures and videos must not be taken of students, teachers or other individuals without their permission. No pictures or video that may denigrate and/or humiliate another student or that constitutes “sexting” or that are lewd may be taken. Pictures or videos of another student, teachers or other individuals may not be uploaded to the Internet or other public venue without their permission
5. The use of vulgar, derogatory, or obscene language while using a mobile device will not be allowed and will face disciplinary action.
6. Mobile devices are not to be taken into restroom areas and used in a manner that does not comply with the AUPMD.
7. Students with repeated infractions of the AUPMD may face increased disciplinary actions, including loss of mobile device privileges.
8. Any student/s caught using a mobile device to cheat in exams or assessments will face disciplinary action.
9. Any use of the mobile device that is deemed a criminal offense, will be dealt with as such by the District.

District’s Responsibilities

1. The District will provide a safe, filtered network according to the Children’s Internet Protection Act and make a best effort attempt to ensure all students will access the Internet through this network.
2. The District will monitor all activity, either Internet access or intranet access.
   The District will make determinations on whether specific uses of the mobile device are consistent with the District’s AUPMD.
3. The Superintendent or their designee will deem what is appropriate for use of mobile devices on district property or on the district’s wireless network.
4. If the District has reasonable cause to believe the student has violated the AUPMD, a student’s mobile device may be searched by authorized personnel.
5. The District may remove the user’s access to the network and suspend the right to use the personal mobile device on district property if it is determined that the user is engaged in unauthorized or illegal activity or is violating the AIPMP. Violation of the AUMD may result in disciplinary action in coordination with the campus Student Code of Conduct.
6. The District assumes no liability or responsibility for students that misuse mobile devices while on school property.
7. The District will educate students in identifying, promoting, and encouraging best practices for Internet safety.