PAUL PUBLIC CHARTER SCHOOL

Paul PCS Internet Use Policy

Internet Usage and Social Media Access

Paul PCS is pleased to make available to students and staff access to interconnected computer systems within the school and to the Internet. In order for the school to be able to continue to make its computer network and Internet access available, all students, staff and guests must take responsibility for appropriate and lawful use of this access. Paul PCS has a no social media access policy for all student devices. Access to social media will be blocked for all students with the support of securly.

Should there be a website that a teacher would like access to, please be sure to submit your request via our ticketing system at paulcharter.gofmx.com to have the website reviewed for access. Requests for access to a blocked website may only be submitted by an adult. Please remember, the ultimate responsibility for monitoring electronic network usage is that of the teachers or staff members using or supervising students using the system.

Acceptable Uses

The school is providing access to its computer networks and the Internet for educational purposes only. The use of your assigned account and school-owned equipment must be in support of education and research and the educational goals of Paul Public Charter School. You are personally responsible for this provision at all times when using the electronic information services.

Privileges

The use of the information system is a privilege, not a right, and inappropriate use of school-owned equipment may result in the cancellation of those privileges. Each person who receives an account will adhere to proper behavior and the use of the network. The Paul Public Charter School Technology Department along with the Director of Operations will determine what appropriate use is . The technology department may close an account at any time when deemed necessary. The administration, staff, or faculty of Paul Public Charter School may request that the IT Manager deny, revoke, or suspend specific user accounts and/or the use of school-owned equipment. Paul Public Charter School makes no warranties of any kind, whether expressed or implied, for the service it is providing.

Paul Public Charter School will not be responsible for any damages suffered while on this system. These damages include loss of data because of delays, nondeliveries, mis-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information

via the information system is at your own risk. Paul Public Charter School specifically disclaims any responsibility for the accuracy of information obtained through its services

Unacceptable Uses

Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

1. Uses that violate the district, state or federal law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by School Policy; view, transmit or download pornographic and gambling materials or materials that encourage others to violate the law; intrude into the networks or computers of others; inappropriate content; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
2. Uses that cause harm to others or damage their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; uploading a worm, virus, "Trojan horse", "time bomb" or other harmful or malicious form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to computers, networks, or information systems.
3. Uses that jeopardize the security and/or quality of student and staff access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user; don't engage in activities that severely degrade the performance of the computer network or other networks on the Internet.
4. Uses that are commercial transactions. Students and staff may not sell or buy anything over the Internet unless deemed necessary in completing their job role. You should not give others private information about you or others, including credit card numbers and social security numbers.
5. Teachers, staff and students are not to use devices that are not assigned to them without the permission of the assigned user of the device or permission from the IT department.

For more details, refer to the Family Handbook.

Social Media Access

Paul PCS has designated networks for Paul Staff, Paul Students and Paul Guest. To increase the security of Paul's networks, Paul's IT department has blocked the access to web content across all networks categorized, listed or containing gambling and adult content. With the increased usage of social media amongst students, the Paul Students network will no longer permit access to social media sites. The designated networks for Paul Staff and Paul Guest will continue to have access to all social media content. Teachers and staff are not to grant students access to the Paul Staff network unless it is required for educational purposes and are solely responsible for the students' use of the staff network.

Internet Access

Internet access is available to use for staff, teachers, students and guests via wired and wireless access. The Paul IT department reserves the right to modify, change or restrict staff's, student's and guest's devices and or access to the Paul's network if deemed necessary for the betterment of the organization. Such restrictions can be from the result of extreme bandwidth strain, violation of Paul's acceptable usage policy and student testing accommodations. Paul grants all teachers and staff the access of a maximum of two devices on the network to ensure sufficient bandwidth is available to meet the needs of the organization.

Paul's network staff will be given the ability to access the staff network through authentication of their provided Windows account information. All school issued devices to teachers will automatically gain access to the staff network. For any personal device a teacher would like to add to the network, it must be approved by the IT department. For connection to the school wireless network, please contact the IT department by our online ticketing system at paulcharter.gofmx.com.

Security

Security on any computer system is a high priority. If you identify a security problem, notify the technology manager at once. Never demonstrate the problem to other users. Never use another person's account without written permission from that person. All use of the system must be under your own account. Any user identified as a security risk will be denied access to the information system. Paul also provides endpoint security protection in the form of Securly, Google Workspace and Microsoft Advanced Threat Protection.

For network security for all devices connected to the network, Paul's Cisco Meraki Firewall is consistently updated with Cisco's threat database to ensure the traffic entering the network is secure at all times. With these systems, Paul's IT Department will monitor the online activities of both scholars and staff and utilize technology security measures during any use of school owned

computers or networks by scholars and adults. The technology protection measures mentioned will block or filter Internet access to sites that are deemed obscene, harmful to students, or not relating to educational content.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy school-owned equipment or the data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to physical damage and the uploading or creation of computer viruses. Writing or drawing is absolutely prohibited on all Chromebooks, laptops and carts at all times. Any vandalism will result in the loss of computer services, disciplinary action, reimbursement of costs of malicious or intentional damages, and legal referral.

Intellectual Property

All data stored on Paul's equipment, softwares, computers or networks is the property of Paul Public Charter School. Additionally, all data created using, sent from and received on the school's electronic computer systems and softwares are, and will remain, the property of Paul PCS. With the utilization of Paul's equipment, softwares, computers and networks, users should expect only limited privacy in the contents of personal files that are not in relation to Paul PCS while on the school's systems.

Student Internet Access

All students will have access to the Internet and World Wide Web information resources only through their school provided classroom devices, student assigned devices or school computer lab. Any special accommodations for the use of the Internet must be approved by the school Principal. Students of Paul PCS will be provided with individual email accounts with approval of their parent or guardian. Students and their parents must sign an agreement to be granted an individual Paul email account.

Paul PCS is a Children's Internet Protection Act (CIPA) compliant school. Under this act, Paul PCS is required to ensure students have blocked or filtered access to pictures and content on student accessible devices that are: (1) harmful to minors; (2) pornography;

and (3) profane. All student online activities will be monitored by Paul PCS as long as students are accessing the internet from the Paul network or from a Paul owned electronic device.

The monitoring of students' activity will be conducted with the support of Google Workspace and Securly's 360 cloud. These systems have been implemented to support Paul's IT department with monitoring students' activity 365 days of the year to ensure our scholars are safe at all times while browsing online.