

Commodore Perry Technology Usage Agreement

Purpose

The purpose of technology, including Chromebooks, laptops, desktops, Internet access, and network usage is to support education and academic research in and among the Commodore Perry School District (CPSD) by providing unique resources and opportunities for collaborative work for students and staff. It is important for parents and students to understand the appropriate use and responsibilities that are associated with this opportunity.

Definition

The CPSD computer network includes all Local Area Networking and Wide Area Networking within the school community as well as all on-line, direct-wired, and wireless networking such as the Internet and the current Internet Service Provider to which the school network is linked. Any personal hardware brought to school that is used on the CPSD network can be procured in the event of a legal matter.

Authority and Access

The CPSD reserves the right to log network use and to monitor file server space utilization by District users. It is often necessary to access user accounts in order to perform routine maintenance and security tasks. User accounts are the property of the School District. The students should have no expectations of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the school computer network or stored in his/her directory. The school's computer network system operator, or other authorized school employee, may, at any time, review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted, reporting any violation of rules to the school administration or law enforcement official if deemed necessary. The District reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity if this activity is discovered.

Guidelines

Users of computer networks have certain privileges, rights and responsibilities. General guidelines for use are provided within this agreement, which shall be signed by all students who use the network. In general, these require efficient, ethical and legal utilization of the network resources. The use of network resources, including the Internet, is a privilege, not a right for students, and inappropriate use shall result in a termination of those privileges.

Security

System security is protected through the use of a "password." Failure to adequately protect or update passwords could result in unauthorized access to personal or District files. To protect the integrity of the system, the following guidelines shall be followed:

- Students will not reveal or share their passwords to anyone other than an authorized technician, homeroom teacher, or school administrator.
- Users are not to use any technology that is currently logged in under another user's account. This includes family members who are employed at or attending Commodore Perry School District.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network for an indefinite period of time.
- Any user attempting to bypass security using a proxy server will be denied access to the network for an indefinite period of time.
- No student user will be granted a "higher" level of access than other users on the system.

Safety and Protection of Personal Information

When sending electronic messages, students will not include personal information, such as addresses, phone numbers, or Social Security numbers that could identify themselves or other students. Internet ID and passwords provided only for personal use within the District. Students will not use anyone else's password, regardless of how the password was obtained. Those who suspect that someone has discovered their password will change it immediately. The authorized CPSD technician has the right to disable or disallow accounts in the event that someone else has taken over their account. Students will not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users. Any student caught violating another student's privacy or a CPSD employee's privacy will have their access to the network fully revoked or denied for a period of time set by the CPSD administration.

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication.

- Any network user who receives threatening or unwelcome communications will immediately bring them to the attention of an administrator or the authorized technicians.
- Network users should not reveal personal addresses, telephone number or Social Security numbers to other users on the network or users on the Internet. **If a user does this and has signed this agreement, the CPSD, its employees, and contracted technicians become exempt from legal action taken against them.**

Acceptable Use

The use of the computer network must be in support of education and research and consistent with the educational objectives of the CPSD. Use of network and computer resources must comply with rules appropriate for that network. Network accounts are to be used only by the authorized user of the account for agreed upon usage and authorized purposes. The determination as to whether a use is appropriate lies solely within the discretion of the CPSD administrators and authorized technicians.

The use of the computer network for illegal, inappropriate or unethical purposes by students is prohibited. More specifically, the following uses are prohibited:

1. Use of the network to facilitate illegal activity.
2. Use of the network for non-school or non-work related activities.
3. Use of the network for product advertisement, political lobbying, commercial, or for-profit purposes.
4. Use of the network for hate mail, vulgar mail, discriminatory remarks, and offensive or inflammatory communication. This includes chat rooms, web posting, blogs, on-line journals, e-mail, and other future communication technologies.
5. Use of the network to transmit material likely to be offensive or objectionable to recipients. This includes email containing vulgar or inappropriate language and material.
6. Use of the network to transmit, access, or obtain obscene, sexually explicit or pornographic material.
7. Use of the network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.
8. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials. This includes audio and video files (MPGs, AVIs, MP#,s, WMAs, etc.).
9. Quoting person communications in a public form without the original author's prior consent.
10. Downloading, installing, or use of unauthorized games, program files, electronic media, or other non-district registered software.
11. Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users.
12. Impersonation of another user, anonymity and pseudonyms.
13. Destruction, modification, or abuse of network hardware and software to disrupt the work of other users.
14. Use of the Internet to access their personal e-mail during school hours for non-school work purposes.
15. Non-teacher sanctioned or authorized game playing is strictly forbidden within the building.

Copyright Infringement

Students will not:

1. Copy and forward, or
2. Copy and download, or
3. Install to the network or Internet server any copyrighted material without the approval by an Administrator, teacher or authorized technician. Copyrighted material is anything written by someone else including but not limited to: games, a story, music, or video files, an encyclopedia entry, or software.

Commercial use

Students will not use the District’s computer network to solicit sales or conduct business (e.g, by posting an advertisement to a news group or by setting up web pages to advertise or sell a service unless specifically required by a teacher for a class project).

Consequences for Inappropriate Use

1. The network user will be responsible for damages to the equipment, systems and software resulting from deliberate or willful acts.
2. Failure to follow the procedures and prohibited uses previously listed in this agreement will result in the loss of network/technology access. Other appropriate disciplinary action may also follow.
3. The following violations will be reported to the appropriate legal authorities for possible prosecution: Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; theft of services.

All Commodore Perry School students have been granted access to our technology and network via a username and password. Tied into these accounts is access to the Internet. This agreement is not only used to help protect the CPSD but also to protect the children. The student’s agreement will be kept on file until either a new agreement is distributed or the parent requests a change in their son/daughter(s) technology access status. All new students will be given a copy of this form to read, complete, and return. A copy of this form can be found at <http://cppanthers.org/> under the “Resources” tab.

Please detach this portion and return it to your first period teacher.

I have read and understand the Commodore Perry Technology Usage Agreement.

_____	_____	_____
Student name	Student Signature	Date

_____	_____	_____
Parent/Guardian name	Parent/Guardian Signature	Date

What is the responsibility of the Commodore Perry School District regarding Internet access and students?

In 2000 Congress enacted the Children's Internet Protection Act (CIPA). Pennsylvania was one of twenty-five states that have Internet filtering laws that apply to publicly funded schools or libraries. It requires school boards and publicly-funded libraries to adopt and enforce acceptable use policies for Internet access that include the (1) use of software programs reasonably designed to block access to visual depictions of obscenity, child pornography or material that is harmful to minors; or (2) selection of online servers that block access to visual depictions of obscenity, child pornography or material that is harmful to minors.

CPSD is in compliance with CIPA and employs the most updated software to ensure safety. While the filter runs 24/7, it is always a possibility that an inappropriate website may make it through the filter. In such an event, the student should not remain on the site and immediately report the incident to his or her teacher.

Personal Technology

If any personal technology is connected to the CPSD's network, it can legally be considered part of the CPSD's property. The content on personal technology can be procured and/or confiscated by the District if the material on them is illegal or improper.