PENNSYLVANIA DISTANCE LEARNING CHARTER SCHOOL

Book:	**Policy Manual**
Section:	**Programs**
Title:	**Technology and Internet Acceptable Usage Policy**
Adopted:	**May 24, 2004**
Revised:	**December 10, 2007, March 3, 2014, March 6, 2019, May 6, 2024**

PURPOSE: Pennsylvania Distance Learning Charter School (PDLCS) is dedicated to providing services and educational programs using current technology necessary for providing a safe and orderly environment and protecting the health, safety, and welfare of all students.

The Internet as used by students and staff of PDLCS will be solely a tool to facilitate educational programs and research. No other use of the Internet will be endorsed or allowed by PDLCS. Specifically, through the use of computers, students and staff will be able to access educational research materials stored on other computers at other facilities located throughout the world. They will also be able to collaborate with other students and peers with Internet access globally.

Although this represents a significant opportunity, there are important responsibilities that must be shared among students, parents and staff. The purpose of this policy is to detail these responsibilities in a manner understandable to all parties involved.

DETAILED POLICY STATEMENT:

COMPUTER NETWORK: PDLCS computer network includes all local area networking and wide area networking within the school community as well as all online and direct-wired networking such as Internet to which the PDLCS network may be linked.

> **ACCEPTABLE USE:** All persons (students and staff) using PDLCS's computer network must conduct themselves in a responsible, ethical and polite manner. Students and staff of PDLCS shall practice responsible computing. Responsible computing encompasses the ethical use of computers and mobile devices as tools. Users of PDLCS's IT resources must adhere to the following principles:
>
> > **1. Legal and Ethical Use**: Users shall use IT resources in a manner consistent with all applicable laws, regulations, and ethical standards. This includes, but is not limited to, refraining from engaging in any unlawful or fraudulent activities.
> >
> > **2. Network Security:** Users shall not attempt to compromise the security of IT resources, including unauthorized access, hacking, or distribution of malicious software.

Users are responsible for maintaining the confidentiality of their passwords and access credentials.

3. Data Privacy: Users shall respect the privacy of others' data and information. Unauthorized access, sharing, or disclosure of sensitive data is strictly prohibited.

4. Copyright and Intellectual Property: Users must respect copyright and intellectual property rights when using IT resources. Unauthorized distribution, reproduction, or sharing of copyrighted materials is prohibited.

5. Responsible Content: Users shall not create, access, download, or distribute offensive, obscene, or inappropriate content through IT resources. This includes, but is not limited to, hate speech, harassment, and material that may be considered discriminatory or defamatory.

UNACCEPTABLE USES: PDLCS's Network is to be used for legitimate academic and employment related purposes only. The following types of access are considered to be inappropriate uses. This list is by no means exclusive and PDLCS reserves the right, at its sole discretion, to determine whether a particular use is considered inappropriate or unacceptable.

1. Accessing profane or obscene material, material suggesting illegal acts and material advocating violence or discrimination.
2. Using the access for illegal acts.
3. Attempts to access any resources that are restricted, confidential or privileged.
4. Posting chain letters.
5. Internet Relay Chat, news groups, or mailing list participation unless directed and supervised by a staff member for a classroom assignment.
6. Unauthorized Access: Attempting to gain unauthorized access to systems, data, or accounts, or attempting to impersonate another user.
7. Granting Internet or Network access to unauthorized persons intentionally or unintentionally, or failing to notify a teacher or administrator if you suspect someone of using your password.
8. Posting personal contact information.
9. Agreeing to meet someone met online without parental approval and under the supervision of a teacher or authorized adult.
10. Attempts to disrupt access.
11. Causing damage to or changing function, operation or design of technology.
12. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening language.
13. Harassing another person.
14. Posting false or defamatory information.
15. Plagiarizing information found on the Internet.
16. Disregarding the rights of copyright owners on the Internet.
17. Posting web pages without the consent of a teacher or authorized adult.

18. Conducting business unrelated to PDLCS.
19. Buying or selling any products or services.
20. Engaging in acts of bullying, harassment, intimidation, and/or threatening conduct including, but not limited to such conduct committed or furthered by means of an electronic act.
21. Using school provided devices to send, receive, or in any way access sexually explicit pictures and messages.
22. Gambling
23. Cybersecurity Threats: Engaging in any activity that may compromise the security and availability of IT resources, including but not limited to hacking, virus distribution, and phishing.
24. Network Abuse: Excessive use of network resources, including bandwidth, which may degrade network performance for others.
25. Using Artificial Intelligence in an unauthorized or unethical manner. This includes but is not limited to acts of academic dishonesty, and the creation of deep fake or shallow fake images or videos.

Students or staff who engage in such activities, or any others deemed inappropriate by PDLCS, shall be subject to disciplinary measures, as deemed appropriate by PDLCS administration, its Board of Trustees and PDLCS policy.

As stated above, use of the PDLCS computer network is to be limited to legitimate academic purposes. This means using the network in such a manner as to have a direct or indirect impact on the student's educational program at PDLCS. The use of computer network for sending frivolous electronic mail (e-mail), chatting, reading, and sending jokes, researching non-academic related sources such as MTV, sports sites, social networking sites such as Facebook, and playing computer games will not be supported or allowed to occur at PDLCS. The use of the system for defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, and illegal material or other prohibited activities shall not be permitted, and PDLCS will use any and all efforts, within the confines of the law, to prevent such material from entering the school's network. Individuals are encouraged to report such activity to the school administration. PDLCS also requires adherence to certain rules for use of its hardware:

1. Learn how to use the hardware properly.
2. Do not adjust, connect, or disconnect components without supervision unless you understand what you are doing and are authorized by PDLCS personnel to do so.
3. Do not connect your personal hardware to PDLCS's hardware.
4. No food or drink within 10' of computer stations.

PRIVACY: For the protection of our students, all users are advised and should be reinforced by parents/guardians to NEVER disclose personal information over the network or Internet, including but not limited to, home address, physical description, age, route to and from a location, or any other personal information that could threaten the safety, identity, and security of our students.

Electronic information and communication sent to, received by, or accessed on PDLCS-owned property, networks, and/or hardware, remain the property of PDLCS. PDLCS reserves the right to monitor electronic activities and communications.

COLLECTION, USE AND DISCLOSURE OF INFORMATION: PDLCS employs the Google Apps suite of products for student use. These applications are powered by Google but administered by PDLCS. Google Apps integrates with the school's standard web single sign-on system using the SAML2.-standard. These single sign-on systems are owned by PDLCS and housed in a secure datacenter within the school. Such systems permit students to access Google Apps only after their school-assigned credentials are authenticated by the systems.

PDLCS student email is provided as part of Google Apps. PDLCS utilizes a set of security tools that allow the school to restrict electronic communications to within the PDLCS domain or school-affiliated domains. PDLCS provides Google Apps and student email accounts to students for educational purposes only. PDLCS is the sole owner of user data. The Google Apps Terms of Service assures PDLCS that the controls, processes and policies that protect user data in Google's system adhere to strict auditing standards; and that Google complies with applicable laws and regulations, including but not limited to applicable privacy laws and the Family Education Rights and Privacy Act (FERPA).

GOOGLE G SUITE ACCOUNT USAGE: The Google G Suite for Education is utilized across all aspects of the school for educational purposes in grades K-12. This account will potentially provide the student's name to Google G Suite Applications and other third party applications. Parents/Guardians consent to the creation of a Google G Suite account for all students of PDLCS to be utilized for school communication, lesson activity completion and as a means for logging into third part educational applications that utilize a Google account single sign on protocol.

GOOGLE APPS: Google Docs is a component of Google Apps. It is a collaborative tool that allows multiple users to collaborate on a single document in real time. PDLCS teachers or staff may assign students to use Google Docs to collaborate on assignments or projects. Students are to use this application for these purposes only. Using Google Docs for unauthorized communication with other students such as passing notes is unacceptable and will not be permitted.

WEBCAM: With technology advancing at such a rapid pace, it is important that we offer our students the tools needed to get the most out of their educational experience. With the growing use of video collaboration tools in schools, PDLCS may choose to offer webcams to some students. PDLCS webcams may be used for face-to-face video meetings between students and staff or parents and staff. They may also be used as educational tools as directed by School Administration. These webcams may be external USB devices that can be connected to student computers as needed or built into the school issued computer. It is the personal responsibility of each student and staff member to use webcams in an appropriate manner, in accordance with the acceptable usage outlines on Page 1 of this policy. PDLCS does not employ the use of webcams to help enforce any polices or asset tracking, nor does the school use webcams to remotely monitor end use activity.

TABLETS: PDLCS is committed to providing a learning environment that will enable students to succeed in a constantly evolving technological landscape. The School believes in the importance of providing students with the 21st century skills they need to become self-motivated learners. To accomplish this vision, PDLCS may choose to loan tablet devices to some students. The following guidelines must be adhered to:

1. Students are expected to use tablets appropriately for educational purposes.
2. Students should not attempt to change the configuration of the devices or removed installed profiles.
3. Chrome Web Store free apps may be installed; however, only those free apps with an app store age appropriate level may be installed.
4. PDLCS will not reimburse for any paid app.
5. PDLCS will not reimburse for mobile coverage.

Tablets will be pre-configured and enrolled on the PDLCS mobile device management server before being assigned to students. This enrollment allows for asset management, as well as remote updates of any PDLCS in-house apps that may be distributed to students. The server also alerts school administration when a tablet has had unauthorized changes made to any installed configuration such as removal of profiles or restrictions. Restrictions will be implemented on each tablet. CIPA-compliant Internet filtering will be installed similar to laptop filtering. This filter is a Web browser that replaces a tablet's default browser on PDLCS tablets. Devices like a tablet can be a valuable tool to encourage students to use technology to research, explore, and be creative. Such tools also support the mission of PDLCS.

NETWORK SECURITY: Using the guidelines of the U.S. Children's Internet Protection Act of 2000, PDLCS has implemented a technology protection measure (Internet site filtering software) to prevent all users of the network from accessing inappropriate Internet sites. Inappropriate Internet sites: include the following content: Anything that falls under at least one of the categories below shall be blocked/filtered. This list will be updated/modified as required.

NUDITY/PORNOGRAPHY:

1. Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
2. Provocative semi-nudity (i.e., lingerie models)
3. Sites which include pornography or links to pornographic sites
4. **Exceptions:** Classical nudity (e.g., Michelangelo), swimsuit models

SEXUALITY:

1. Sites which contain material of a mature level (elementary/middle school levels)
2. Images or descriptions of sexual aids
3. Descriptions of sexual acts or techniques
4. Sites which contain inappropriate personal ads

VIOLENCE:

1. Sites which promote violence
2. Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
3. Graphic autopsy or crime-scene images

CRIME:

1. Information on performing criminal acts (e.g. drug or bomb making, computer "hacking")
2. Illegal file archives (e.g., software privacy)

DRUG USE:

1. Sites which promote the use of illegal drugs
2. Materials advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
3. **Exception:** Material with valid-educational use (e.g., drug-use statistics)

Student Hardware PDLCS Students will be issued the necessary computer and peripheral devices necessary to facilitate their learning upon enrollment. Students are required to use only school-owned and issued technology, including but not limited to Chromebooks, laptops, software, and other peripherals, to complete school activities.

In the event of any issues or malfunctions with the technology, Parents/Guardians or Students should first attempt to troubleshoot the problem using provided resources or contacting the IT department for remote assistance.

If the issues cannot be resolved remotely, IT will coordinate with the Materials Coordinator to ship a replacement device, along with provisions for the family to ship the broken device back to the school. PDLCS families should return the broken devices within 3 business days of receiving the return shipment labels. It is important to return broken devices promptly, as students that have multiple devices assigned to them may not be shipped additional replacement devices until previously assigned devices are returned to the school.

Employee Hardware PDLCS employees will be issued the necessary computer and peripheral devices for the completion of their job duties. Employees are required to use only school-owned and issued technology, including but not limited to computers, laptops, mobile devices, software, and peripherals, to perform their job responsibilities.

Personal devices and software are prohibited for conducting school business, unless explicitly approved by a PDLCS Chief Officer.

In the event of any issues or malfunctions with the technology during remote work days, employees should first attempt to troubleshoot the problem using provided resources or contacting the IT department for remote assistance. If the issue cannot be resolved remotely, employees are required to report to the office for further assistance.

Employees should promptly notify their supervisor if they encounter technology-related issues that prevent them from fulfilling their job duties effectively while working remotely.

Reporting Violations Users are encouraged to report any suspected violations of this AUP to the Chief Operations Officer, or to Technical Support (888-997-3352 Option 2/support@padistance.org). Reports will be treated confidentially to the extent permitted by law.

Policy Review PDLCS reserves the right to modify this Acceptable Use Policy at any time. Users are responsible for reviewing and understanding the most current version of this policy.

By using PDLCS's IT resources, users acknowledge that they have read, understood, and agreed to comply with this Acceptable Use Policy.