Providence Hall Charter School

Herriman, UT 84096 Phone: 801.727.8260 providencehall.com

5000 - Students
50 - Electronic Device & Acceptable Use Policy

1. <u>Electronic Devices</u>

1.1. Electronic devices include <u>but are not limited to</u>

1.1.1. cell phones,

1.1.2. iPods,

1.1.3. iPhones,

1.1.4. digital music players,

1.1.5. iPads,

1.1.6. digital readers,

1.1.7. laptops, and

1.1.8. electronic gaming devices.

1.2. Students may use electronic devices on campus before or after school hours as well as in the hall between classes.

1.3. Students are also permitted to use electronic devices during lunchtime as long as they do not cause a distraction or disruption, or cause the student to be tardy to their next class period.

1.4. Students should not use any electronic devices in the classroom except under the direction of the teacher and for educational purposes.

1.5. Teachers will include in their class syllabus any additional and specific guidelines governing the use of electronics in their specific classrooms.

1.6. Providence Hall Charter School (PHCS) administration will support any pre-approved specific classroom electronic device usage policy.

1.7. The following consequences apply to all students who choose not to follow PHCS's electronic device use policies.

1.7.1. ***1st Offense***: Electronic Device is confiscated from students, placed in the office, and returned to the student at the end of the school day with a warning.

1.7.2. ***2nd Offense***: Electronic device is returned to student after two (2) school days and parent/guardian contact.

1.7.3. ***3rd Offense***: Electronic device is returned to student after three (3) school days and a parent/guardian and student conference with administration

1.7.4. ***4th Offense***: Electronic device is returned to students after four (4) school days and loss of school activities/privileges for thirty (30) days. Students may also serve detention.

1.7.5. ***5th Offense and Beyond***: Electronic device is only returned to a parent/guardian after five (5) school days and may result in suspension from school.

1.8. Per Utah Code A§ 76-10-1206, it is illegal to produce and/or distribute any material that inappropriately portrays a minor. This includes taking or distributing inappropriate pictures or videos of other students regardless of whether it is consensual. PHCS will follow the State of Utah's designated protocol when dealing with matters of illegal production or distribution of material through phone, computer, or other electronic device. Students in violation of this policy will be subject to administrative actions.

1.9. Students refusing to surrender their personal electronic devices to any PHCS employee when asked will be subject to PHCS discipline and will lose the privilege of having electronic devices at school for a period of not less than five (5) days and a parent/guardian will be notified.

1.10. Students are limited to a maximum of TWO (2) devices brought from home that access the school's wifi. If students bring more than two (2) devices they may be removed from the network, and subject to possible disciplinary measures.

2. Acceptable Use

PHCS recognizes the value of computers and other electronic resources to improve student learning and enhance the administration and operation of its schools. To this end, PHCS encourages the responsible use of computers; computer networks, including the Internet; and other electronic resources in support of the mission and goals of PHCS and its schools. The Internet is an unregulated and a worldwide vehicle for communication; making information, available to PHCS employees and students, impossible to control. Therefore, the PHCS Board of Trustee (Board) adopts this policy governing the voluntary use of electronic resources and the Internet in order to provide guidance to individuals and groups obtaining access to these resources on PHCS-owned equipment or through PHCS-affiliated organizations.

2.1. Acceptable Use

2.1.1. All use of the Internet must be in support of educational and research objectives consistent with the mission and objectives of PHCS.

2.1.2. Proper codes of conduct in electronic communication must be used. In newsgroups, giving out personal information is inappropriate. When using e-mail, extreme caution must always be taken in revealing any information of a personal nature.

2.1.3. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.

2.1.4. All communications and information accessible via the network should not be assumed to be private property.

2.1.5. Subscriptions to mailing lists and bulletin boards must be reported to the system administrator. Prior approval for such subscriptions is required for PHCS employees and students.

2.1.6. Mailing list subscriptions will be monitored and maintained, and files will be deleted from the personal mail directories to avoid excessive use of file server hard-disk space.

2.1.7. Exhibit exemplary behavior on the network as a representative of your school and community. Be polite!

2.1.8. From time to time, PHCS Administration will make determinations on whether specific uses of the network are consistent with the acceptable use practice.

2.2. Unacceptable Use

2.2.1. Giving out personal information about another person, including home address and phone number, is strictly prohibited.

2.2.2. Any use of the network for commercial or for-profit purposes is prohibited.

2.2.3. Excessive use of the network for personal business shall be cause for disciplinary action.

2.2.4. Any use of the network for product advertisement or political lobbying is prohibited.

2.2.5. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.

2.2.6. No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.

2.2.7. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

2.2.8. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.

2.2.9. The unauthorized installation of any software, including shareware and freeware, for use on PHCS's computers is prohibited.

2.2.10. Use of the network to access or process pornographic material, inappropriate text files (as determined by the system administrator and/or building administrator), or files dangerous to the integrity of the local area network is prohibited.

2.2.11. PHCS's network may not be used for downloading entertainment software or other files not related to the mission and objectives of PHCS for transfer to a user's home computer, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of PHCS.

2.2.12. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).

2.2.13. Use of the network for any unlawful purpose is prohibited.

2.2.14. Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.

2.2.15. Playing games is prohibited unless specifically authorized by a teacher for instructional purposes.

2.2.16. Establishing network or Internet connections to live communications, including voice and/or video (relay chat), is prohibited unless specifically authorized by the system administrator.

3. PHCS Rights and Responsibilities

It is the policy of the PHCS to maintain an environment that promotes ethical and responsible conduct in all online network activities by PHCS employees and students. It shall be a violation of this policy for any PHCS employee, student, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of the network. Within this general policy, the PHCS recognizes its legal and ethical obligation to protect the well-being of students in its charge. To this end, PHCS retains the following rights and recognizes the following obligations:

3.1. Rights & Obligations

3.1.1. To log network use and to monitor fileserver space utilization by users, and assume no responsibility or liability for files deleted due to violation of fileserver space allotments.

3.1.2. To remove a user account on the network.

3.1.3. To monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.

3.1.4. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to PHCS-owned equipment and, specifically, to exclude those who do not abide by the PHCS's acceptable use policy or other policies governing the use of school facilities, equipment, and materials. PHCS reserves the right to restrict online destinations through software or other means.

3.1.5. To provide guidelines and make reasonable efforts to train PHCS employees and students in acceptable use and policies governing online communications.

3.2. ***PHCS Employee Responsibilities***

3.2.1. PHCS employees who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the PHCS.

3.2.2. PHCS employees should make reasonable efforts to become familiar with the Internet and its use so that effective monitoring, instruction, and assistance may be achieved.

3.3. ***User Responsibilities***

3.3.1. Use of the electronic media provided by the PHCS is a privilege that offers a wealth of information and resources for research. Where it is available, this resource is offered to PHCS employees, students, and other patrons at no cost. In order to maintain the privilege, users agree to learn and comply with all of the provisions of this policy.

4. Disclaimer

4.1. PHCS cannot be held accountable for the information that is retrieved via the network.

4.2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

4.3. PHCS will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.

4.4. PHCS makes no warranties (expressed or implied) with respect to:

4.4.1. the content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information; and

4.4.2. any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.

4.5. No expectation of privacy applies to all network usage on the PHCS networks.

4.6. PHCS reserves the right to change its policies and rules at any time.

5. Agreement & Signature

5.1. *User Agreement (to be signed by all adult users and student users K-12 unless age 18 or above in Skyward).*

5.1.1. I have read, understand, and will abide by the above Electronic Device and Acceptable Use Policy when using computer and other electronic resources owned, leased, or operated by the PHCS. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

5.2. *Parent/Guardian Agreement (to be signed in Skyward by parents/guardians of all student users under the age of 18)*

5.2.1. As a parent/guardian, I have read the Electronic Device and Acceptable Use Policy. I understand that this access is designed for educational purposes. PHCS has taken reasonable steps to control access to the Internet, but cannot guarantee that all controversial information will be inaccessible to student users. I agree that I will not hold PHCS responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my student to use network resources, including the Internet, that are available through PHCS.

5.2.2. Agreements must be signed by the 20th day of the school year or 20th day of the beginning of enrollment for transfer students, whichever is earlier.

6. <u>Electronic Mail Guidelines</u>

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal. You should understand the following:

6.1. PHCS provides electronic mail to PHCS employees and students to enable them to communicate effectively and efficiently with one another for the purpose of educational needs.

6.2. ***When using the PHCS' electronic mail facilities you should comply with the following guidelines.***

6.3. If you are in any doubt about an issue affecting the use of electronic mail, you should consult the IT Director.

6.4. Any breach of these guidelines may lead to disciplinary action.

6.5. DO...

6.5.1. Do check your electronic mail daily to see if you have any messages.

6.5.2. Do include a meaningful subject line in your message.

6.5.3. Do check the address line before sending a message and confirm you are sending it to the right person.

6.5.4. Do delete electronic mail messages when they are no longer required.

6.5.5. Do respect the legal protections to data and software provided by copyrights and licenses.

6.5.6. Do take care not to express views that could be regarded as defamatory or libelous.

6.5.7. Do use an "out of the office assistant" to automatically reply to messages when you are not available.

6.6. DO NOT...

6.6.1. Do not print electronic mail messages unless absolutely necessary.

6.6.2. Do not expect an immediate reply; recipients might not be at their computer or could be too busy to reply straight away.

6.6.3. Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.

6.6.4. Do not use electronic mail for personal reasons.

6.6.5. Do not send excessively large electronic mail messages or attachments.

6.6.6. Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to multiple people.

6.6.7. Do not participate in chain or pyramid messages or similar schemes.

6.6.8. Do not represent yourself as another person.

6.6.9. Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive, or libelous.

6.7. Please note the following:

6.7.1. All electronic mail activity is monitored and logged.

6.7.2. All electronic mail coming into or leaving the organization is scanned for viruses.

6.7.3. All the content of electronic mail is scanned for offensive material.

7. Password Guidelines

7.1. Overview

7.1.1. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of PHCS's entire network. As such, PHCS employees (including contractors and vendors with access to PHCS systems) and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

7.2. Purpose

7.2.1. The purpose of these guidelines are to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

7.3. Scope

7.3.1. The scope of these guidelines includes all PHCS employees and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any PHCS facility, has access to the PHCS network, or stores any non-public PHCS information.

7.4. Policy

7.4.1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

7.4.2. All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six (6) months. The recommended change interval is every four (4) months.

7.4.3. Each successive password must be unique. Re-use of the same password will not be allowed.

7.4.4. Passwords must be a minimum of eight (8) characters long.

7.4.5. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

7.4.6. Passwords must not be inserted into e-mail messages or other forms of electronic communication.

7.4.7. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

7.4.8. All user-level and system-level passwords must conform to the guidelines described below.

7.4.9. Passwords should never be written down or stored online.

7.5. Password Construction Guidelines

Passwords are used for various purposes at the PHCS. Some of the more common uses include: user-level accounts, web accounts, email accounts, screen saver protection, voice-mail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

7.5.1. Poor (unacceptable) passwords have the following characteristics:

7.5.1.1. The password contains fewer than eight (8) characters.

7.5.1.2. The password is a word found in a dictionary (English or foreign).

7.5.1.3. The password is a common usage word such as:names of family, pets, friends, co-workers, fantasy characters, etc.

7.5.1.4. The password is computer terms and names, commands, sites, companies, hardware, software, etc.

7.5.1.5. The password is acronyms for the agency or city.

7.5.1.6. The password is birthdays and other personal information such as addresses and phone numbers.

7.5.1.7. The password is a word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

7.5.1.8. The password is any of the above spelled backwards.

7.5.1.9. The password is any of the above preceded or followed by a digit (e.g., secret1, 1secret)

7.5.2. Strong (acceptable) passwords have the following characteristics:

7.5.2.1. Contain both upper and lowercase characters (e.g., a?z *and* A?Z).

7.5.2.2. Have digits and punctuation characters as well as letters (e.g., 0?9 *and* !@#$%ˆ&*()_+|~--=\`{}[]:";í<>?,./).

7.5.2.3. Are at least eight (8) alphanumeric characters long.

7.5.2.4. Are not a word in any language, slang, dialect, jargon, etc.

7.5.2.5. Are not based on personal information, names of family, etc.

7.5.2.6. Can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

7.6. Password Protection Standards

7.6.1. Do not use the same password for PHCS accounts as for other non-PHCS access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for the various PHCS access needs. For example, select one password for the e-mail systems and a separate password for network systems.

7.6.2. Do not share PHCS passwords *with anyone*, including other students, teachers, administrative assistants, or secretaries. All passwords are to be treated as sensitive, confidential PHCS information.

7.6.3. If someone demands a password, refer them to this document or have them call someone in the IT Department.

7.6.4. Do not write passwords down and store them anywhere in your office or classroom. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

7.6.5. Change passwords at least once every six (6) months (except system-level passwords which must be changed quarterly). The recommended change interval is every four (4) months.

7.6.6. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

7.6.7. The IT Department or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

7.7. Use of Passwords and Pass-Phrases for Remote Access Users

Access to the PHCS networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass-phrase.

7.7.1. Pass-Phrases

7.7.1.1. Pass-phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all and the private key that is known only to the user. Without the pass-phrase to "unlock" the private key, the user cannot gain access.

7.7.1.2. Pass-phrases are not the same as passwords. A pass-phrase is a longer version of a password and is, therefore, more secure.

7.7.1.3. A pass-phrase is typically composed of multiple words. Because of this, a pass-phrase is more secure against "dictionary attacks." A good pass-phrase is relatively long and contains a combination of upper- and lowercase letters and numeric and punctuation characters. An example of a good pass-phrase is: "The###TrafficOnThe101Was***ThisMorning." All of the rules above that apply to passwords apply to pass-phrases.

8. Enforcement

Any PHCS employee or student found to have violated this policy may be subject to disciplinary action and loss of network privileges.