

Philadelphia Academy Charter School

Elementary Program (K-8)
11000 Roosevelt Blvd.
Philadelphia, PA 19116
Tel: (215) 676-8320
Fax: (215) 676-8340



High School Program (9-12)
1700 Tomlinson Rd.
Philadelphia, PA 19116
Tel: (215) 673-3990
Fax: (215) 673-3341

www.pacsweb.org

Acceptable Use Policy for the Exploration and Utilization of the Internet As a Tool for Learning by Students and Staff

Purpose

The Charter School relies on its computer network to conduct business and student learning. To ensure appropriate use of the School's Computer Resources, the Philadelphia Academy Charter School (the "School") has created this Computer Usage Policy (the "Policy").

It is every computer User's (as defined below) duty to use the Computer Resources responsibly, professionally, ethically and lawfully. Access to these resources may be designated a privilege not a right.

DEFINITIONS

From time to time in this Policy, we refer to terms that require definitions:

The term "**Computer Resources**" refers to the School's computer network. Specifically, Computer Resources, whether owned or leased, including, but not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, web servers, workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example: Internet commercial online services, value-added networks, e-mail systems) that may be accessed directly or indirectly from our computer network.

The term "**Users**" refers to all employees, independent contractors, consultants, temporary workers, students, family members, and other persons or entities that use our Computer Resources.

POLICY

The Computer Resources are the property of the School. Users are permitted access to the computer system to assist them in the performance of their jobs and academic purposes. Occasional, limited, and appropriate personal use of the computer system is permitted when the use does not: (1) interfere with the User's work performance or academic performance; (2) interfere with any other User's work performance or academic performance; (3) have undue impact on the operation of the computer system; (4) violate any other provision of this policy or any other policy, guideline, or standard of the School. At all times, Users have the responsibility to use Computer Resources in a professional, ethical, and lawful manner.

Use of the computer system is a privilege that may be revoked at any time. In using or accessing our Computer Resources, Users must comply with the provisions that follow.

NO EXPECTATION OF PRIVACY: The computers and computer accounts given to Users are to assist them in the performance of their jobs and for academic purposes. Users do not have an expectation of privacy in anything they create, store, send or receive on the computer system. The computer system belongs to the School and should be used primarily for the School's business and academic purposes.

Monitoring the Online Activities of the Users: Network monitoring tools are used to "police" Computer Resources of all Users. (Examples: VNC, PC Anywhere, Remote Control, and Hyena). Teachers are required to monitor their student's activities, while using the Computer Resources in all learning environments.

WAIVER OF PRIVACY RIGHTS: Users expressly waive any right of privacy in anything they create, store, send or receive on the computer or through the Internet or any other computer network. Users consent to allowing personnel of the School to access and review all materials Users create, store, send or receive on the computer or through the Internet or any other computer network. Users understand that the School may use human or automated means to monitor use of their Computer Resources.

PROHIBITED ACTIVITIES

PROHIBITED USES: Without prior written permission from the School, Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, mass mailings, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material, downloading non-academic related media, plagiarism, hacking or any other unauthorized or illegal use.

INAPPROPRIATE OR UNLAWFUL MATERIAL: Material that is fraudulent, harassing, sexually explicit, pornographic, violent or advocating of violence, profane, obscene, intimidating, threatening, defamatory, discriminatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other forms of electronic communication (such as bulletin board systems, newsgroups, chat groups) or accessed, reviewed, displayed on or stored in the School's Computer Resources. Users encountering or receiving this kind of material have the responsibility to immediately report the incident to their teacher or direct supervisor.

SPOOFING AND SPAMMING: Users may not, under any circumstances, use "spoofing" or other means to disguise their identities in sending e-mail or other electronic communication via bulletin boards, newsgroups or chat groups. Without expressed permission from the School, Users may not send unsolicited ("spamming") e-mails to persons with whom they do not have a prior relationship or bona fide School business purpose.

MISUSE OF SOFTWARE: Without prior written authorization from the School, Users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any independent contractors or clients of the School or to any third person; (3) modify, revise, transform, recast or adapt any software or (4) reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law have the responsibility to immediately report the incident to their teacher or direct supervisor.

COMMUNICATION OF TRADE SECRETS: Unless expressly authorized by the School, sending, transmitting, or otherwise disseminating proprietary data, trade secrets or other confidential information of the School is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties.

OTHER: Unless expressly authorized by the School, the following are also unacceptable uses of Computer Resources, as defined herein:

1. Users may not use Computer Resources to access material that is profane or obscene (pornography of any kind), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
2. Users may not post personal information on the Internet about themselves or other people. Personal contact information includes address, telephone numbers, school address, work address, pictures or video bites, clips, etc.
3. Students may not agree to meet with someone they have met on the Internet without their parent's approval and participation.
4. Users may not attempt to gain unauthorized access to any other computer system. This includes attempting to log-in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing," "snooping" or "electronic discovery."
5. Users may not deliberately disrupt or harm hardware or systems, interfere with computer performance, interfere with another's ability to use equipment and systems or destroy data.
6. Users may not use Computer Resources to engage in illegal acts, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.
7. Users may not use the Computer Resources to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others.
8. Users may not post information that could endanger an individual, cause personal damage or a danger of service disruption.
9. Users may not knowingly or recklessly post false or defamatory information about a person or organization.
10. Users may not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other Users.
11. Users may not indirectly or directly make connections that create "backdoors" to the School, other organizations, community groups, etc. that allow unauthorized access to the Computer Resources or the School.
12. Users may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening or disrespectful language.
13. Users may not engage in personal attacks, including prejudicial or discriminatory attacks.
14. Users may not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
15. Users may not re-post a message that was sent to them privately without permission of the person who sent them the message.
16. Users may not forward or post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.
17. Users will not install or reproduce unauthorized or unlicensed software on Computer Resources.

18. Users may not plagiarize works that they find on the Internet or other resources.
19. Users may not use Computer Resources for private business activities or unreasonable personal use.
20. Users may not use Computer Resources for political lobbying.
21. Students will not download files unless approved by their teacher.
22. Students will follow the directions of their teachers and administrators when using Computer Resources and will obey all school rules regarding Computer Resource usage.

CODE OF STUDENT CONDUCT

Student behavior on Computer Resources is also governed by the behavioral expectations which appear in the School's Code of Student Conduct.

Teachers and other staff members will make every attempt to monitor and guide students toward appropriate materials and the use of the system. It is understood that access to the Computer Resources is a privilege, not a right. Failure to abide by the rules in this document could result in the revocation of access privileges, disciplinary action (including suspension or expulsion from the School), or legal action, as deemed appropriate. Parents/guardians or perpetrators may be billed for damages to equipment. Illegal activities will be referred to the appropriate law enforcement agency. Actions warranting suspension or expulsion will be subject to the due process procedures outlined in the Code of Student Conduct.

PASSWORDS

RESPONSIBILITY FOR PASSWORDS: Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online or given to others without express consent of the Network Administrator. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

PASSWORDS DO NOT IMPLY PRIVACY: Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The School has global passwords that permit access to all material stored on their computer system regardless of whether that material has been encoded with a particular User's password.

SECURITY

ACCESSING OTHER USER'S FILES: Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter or copy a file belonging to another User does not imply permission to read, alter or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other Users by unnecessarily reviewing the files and e-mail.

ACCESSING OTHER COMPUTERS AND NETWORKS: A User's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those

systems or to make use of those systems unless specifically authorized by the administrators of those systems.

COMPUTER SECURITY: Users may not attempt to circumvent the School data protection measures or uncover security loopholes or bugs. Users may not gain or attempt to gain unauthorized access to restricted areas or files on the computer system. Users should not tamper with any software protections or restrictions placed on computer applications, files, or directories. Users who engage in this type of activity may be subject to loss of computer privileges, disciplinary action up to and including expulsion from the School or termination of employment as well as civil and criminal liability.

INTERNET FILTERING TECHNOLOGY: The School employs firewall solutions. At a minimum, it is meant to block visual depictions that are obscene, child pornography, and harmful to minors. If a User finds a website deemed inappropriate, it must be reported to the User's teacher, teacher's administrator and/or Network Administrator. After review of the site, appropriate steps will be taken to shield the site from Users. For purposes of bona fide research or other lawful purposes, certain blocked sites may be made available for those purposes only after approval of the request by the Network Administrator. The School does not warrant the effectiveness of Internet filtering.

VIRUSES

VIRUS DETECTION: Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses to the School's network. To that end, all material received on floppy disk or other magnetic or optical medium and all materials downloaded from the Internet or from computers or networks that do not belong to the School **must** be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops might contain viruses. All disks transferred from home computers and laptops to the School's network **must** be scanned for viruses. Any User receiving e-mail from a questionable source, **must** contact the Network Administrator before opening the e-mail or any attachment included in the e-mail.

ACCESSING THE INTERNET: To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the School's network must do so through an approved Internet firewall.

ENCRYPTION SOFTWARE

USE OF ENCRYPTION SOFTWARE: Users may not install or use encryption software on any of the School computers without first obtaining written permission from the Network Administrator. Users may not use passwords or encryption keys that are unknown to the Network Administrator.

EXPORT RESTRICTIONS: The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States.

E -MAIL

E-MAIL DISPOSAL: Unless directed to the contrary by the Network Administrator, Users should discard inactive e-mail after sixty days. Information subject to federal and/or state laws and regulations governing mandatory retention of records and electronic communication may require you to maintain files or documents for a specified period of time. It is the User's responsibility to know which records are subject to these conditions and to comply with these laws and regulations.

DRAFTING E-MAILS: Because they may appear informal, e-mail messages are sometimes off-hand, like a conversation, and not as carefully thought out as a letter or memorandum. Like any other document, an e-mail message or other computer information can later be used to indicate what a User knew or felt. You should keep this in mind when creating e-mail messages and other documents. Even after you delete an e-mail message or close a computer session, it may still be recoverable and may remain on the system.

MISCELLANEOUS

UNAUTHORIZED DISCLOSURE OF INFORMATION OF MINORS: It is a violation of state laws, including, but not limited to, Title 22 of the Pennsylvania Code and federal laws, including but not limited, to the Family Education Rights and Privacy Act ("FERPA"), to access data of a student you do not directly instruct or to disclose information about a student without parental permission or absent an exception to the disclosure requirements. All access and distribution of student data is recorded. Questions regarding the disclosure of student information must be directed to the CEO prior to disclosure and must conform to the School's student records/confidentiality policies.

PRIVILEGED ATTORNEY-CLIENT COMMUNICATIONS: Confidential e-mail sent from or to in-house counsel or an attorney representing the School should include this warning header on each page:

"ATTORNEY-CLIENT PRIVILEGED: DO NOT FORWARD WITHOUT PERMISSION."

COMPLIANCE WITH APPLICABLE LAWS AND LICENSES: In their use of Computer Resources, Users must comply with all software licenses/copyrights and all other state, federal, and international laws governing intellectual property and online activities. You should not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means, unless you have confirmed in advance from appropriate sources that the School has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the School, as well as legal action by the copyright owner. Any questions concerning these rights should be directed to your teacher, the teacher's administrator or direct supervisor, the Network Administrator or the School's solicitor.

CESSATION OF ACCESS: Upon termination or ending of employment, expulsion from the School, withdrawal from the School, etc., no further access to or use of Computer Resources is permitted without express authorization from the Network Administrator.

NO ADDITIONAL RIGHTS: This Policy is not intended for and does not grant Users any contractual rights.

You MUST complete and return this form to the CEO in order to be granted Internet access. You should make and retain a signed copy for your personal records.

**Philadelphia Academy Charter School School
Acknowledgment of Agreement**

Name _____
(Please Print) (Last) (First) (Middle Initial)

As a User of the School Computer Resources, I have read the entire Acceptable Use Policy, which consists of 6 pages, understand it and agree to comply with the guidelines contained in the Policy as explained by the School and the Network Administrator. In addition to complying with all terms of the Policy, when using any of the School Computer Resources, as defined above, I accept the following basic rules:

1. I will treat all Computer Resources with care and will leave them in good working condition when I am finished.
2. I will use appropriate language on all Computer Resources. If the language is obscene, defamatory, harassing, sexually explicit, threatening, violent, insulting, demeaning or otherwise inappropriate as deemed by a teacher, the teacher's administrator, Network Administrator or the CEO, I will not access it, use it, or disseminate it.
3. I will always treat people on-line with respect. I will not use any of the School Computer Resources to insult or threaten other Users. I assume responsibility for the content of messages I send to others.
4. I will respect the privacy of other Users and will not make any attempts to gain access into the private mailboxes of those Users. I will not allow other Users access to my mailbox and will keep my password private.
5. I understand that Computer Resources are to be used for educational use. I understand that the Network Administrator can access and read my messages.
6. I understand that all Computer Resources belong to the School, and I will treat them with respect.
7. I will not install or download any applications (games), programs or materials at school from the Internet or from any Computer Resources, unless the Network Administrator gives me permission in writing.
8. I will not add any software to the School's Computer Resources unless the Network Administrator gives me permission in writing.
9. I understand that the software provided to me for use is protected under copyright law. I agree not to copy this software unlawfully and/or distribute any materials provided for our use. I will model and encourage ethical use of the software among my friends, family members, and the community.

By signing below, you agree to abide by the Acceptable Use Policy and understand that failure to follow all rules as explained in this document may result in the loss of your privileges to Computer Resources; disciplinary action, including suspension or expulsion from the School; termination of employment; charges for damages; and civil or criminal penalties. You are subject to the punishment determined by the School.

X _____
(Student/Staff Signature) (Date)

X _____
(Parent/Guardian Signature, if applicable) (Date)