Book	Policy Manual
Section	Operations
Title	Acceptable Use and Internet Safety Policy
Code	615
Adopted	October 15, 2020
Revised	September 16, 2021

Board of Trustees Policy

ACCEPTABLE USE AND INTERNET SAFETY POLICY

The Board ("Board") of Trustees of the Chester Community Charter School ("Charter School") provides computer network and Technology Resources to enhance educational opportunities for Charter School students, employees, and the Charter School community. This policy details acceptable use of Technology Resources provided by the Charter School. These services and equipment are provided by the Charter School as a privilege to the User (as defined below) and appropriate and ethical use of any Charter School Technology Resources, tools and equipment is required.

It is every Technology Resource User's duty to use Technology Resources responsibly, professionally, ethically and lawfully. Access to these resources may be designated a privilege, not a right. This policy applies to aspects of both adult and minor acceptable use of Technology Resources.

This policy is intended to fulfill requirements of state and federal laws to the extent applicable, including the Federal Children's Internet Protection Act (CIPA), 47 U.S.C. §§ 254(h) and (l)[1] and the Neighborhood Children's Internet Protection Act (NCIPA)[2], the 2008 Broadband Improvement Act, P.L. 110-385[3] and any applicable implementing regulations. As such, this policy addresses the following:

(A) Access by minors to inappropriate matter on the Internet and World Wide Web;

(B) The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

(C) Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

(D) Unauthorized disclosure, use, and dissemination of personal information regarding minors; and

(E) Measures designed to restrict minors' access to materials harmful to minors.

In using or accessing the Charter School's Technology Resources, Users must comply with the following provisions:

*** This Policy reappears in the "Student" section, Policy #925, for convenience purposes only*

Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined as follows:

Child Pornography. Under federal law, any visual depiction, including any photograph, film, video, picture, or computer image or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C.A. §2256(8)[4]

Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

18 PA CSA §6312(d)[5]

Minor. For purposes of compliance with CIPA, an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean any person under the age of eighteen (18).

Obscene. Under federal and Pennsylvania law, any material if:

1. the average person, applying contemporary adult community standards, would find that the material, taken as a whole, appeals to the prurient interest;
2. the subject matter depicts or describes sexual conduct in a patently offensive way; and
3. the subject matter, taken as a whole, lacks serious literary, artistic, political or scientific value.

Miller v. California, 413 U.S. 15 (1973)[6].

Password. A unique word, phrase or combination of alphanumeric and non-alphanumeric characters used to authenticate a User ID as belonging to a specific User.

Sexual Act and Sexual Contact. Has the meanings given such terms under 18 U.S.C. § 2246(2)[7] 18 U.S.C. § 2246(3)[7], and 18 Pa.C.S.A. § 5903[8].

Technology Protection Measure. A specific technology that blocks or filters Internet access to content that is Obscene, Child Pornography or harmful to Minors and the material is covered by a certification regarding CIPA.

Technology Resources. Technologies, devices and resources used to access, store or communicate information. This definition includes, but is not limited to, computers, information systems, networks, laptops, Chromebooks, iPads, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, digital cameras, wireless reading devices, i.e. Kindles and Nooks, Internet, electronic mail, electronic communications, WIFI, internet access, cloud storage, devices and services, multi-media resources, hardware and software, including Moodle software.

User. Any person who has signed this policy and is permitted by the Charter School to utilize any portion of the Charter School's Technology Resources including, but not limited to, students, parents, employees, Board of Trustee members, contractors, consultants, vendors and agents of the Charter School.

User Identification (ID). Any identifier that would allow a User access to Charter School's Technology Resources or to any program including, but not limited to, e-mail and Internet access.

Vandalism. Any malicious attempt to harm or destroy Technology Resources, data of another user, Internet or other networks. This includes, but is not limited to, the uploading or creation of computer viruses.

Authorized Users

Charter School's Technology Resources may be used by any authorized User. Use of Charter School's Technology Resources is a privilege, not a right. If a potential User has a history of discipline problems involving Technology Resources, the CEO or his/her designee may make the decision not to give the potential user access to certain Charter School Technology Resources.

User Privacy

Computer accounts and Technology Resources are given to Users to assist them in the performance of Charter School related functions. A User does not have a legal expectation of privacy in the User's electronic communications or other activities involving Charter School's Technology Resources, including e-mail, in anything they create, store, send, share, access, view or receive on or through the Internet.

By using Charter School's network and Technology Resources, all Users are expressly waiving any right to privacy and consenting to having their electronic communications and all other use accessed, reviewed and monitored by the Charter School. A User ID with e-mail access will only be provided to authorized Users on condition that the User consents to interception of or access to all communications accessed, sent, received or stored using Charter School technology and signs this policy.

Electronic communications, downloaded material and all data stored on the Charter School's Technology Resources, including files deleted from a User's account, may be intercepted, accessed or searched by the Charter School administrators or designees at any time in the regular course of business to protect Users and the Charter School's equipment. Any such search, access or interception will be reasonable in inception and scope and shall comply with all applicable laws.

Technology Administration

The Board directs the Chief Executive Officer of the Charter School (CEO) or his/her designee to assign trained personnel to maintain the Charter School's technology in a manner that will protect the Charter

School from liability and will protect confidential student and employee information retained on or accessible through the Charter School's Technology Resources.

Administrators may suspend access to and/or availability of the Charter School's Technology Resources to diagnose and investigate network problems or potential violations of the law or the Charter School policies and procedures. All Charter School Technology Resources are considered Charter School property.

The Charter School may maintain or improve Technology Resources at any time. The Charter School or authorized Charter School agents may remove, change or exchange hardware, equipment or other technology between buildings, classrooms or Users at any time without prior notice.

Content Filtering and Monitoring

The Charter School employs technology protection measures and will monitor the online activities of Minors on the Charter School network and/or all Technology Resources and equipment with Internet access, as required by law. At a minimum, they are meant to block visual depictions that are obscene, illegal, pornographic, Child Pornographic and/or harmful to Minors as well as Internet/World Wide Web/computer resource access to such material. If Users find a website deemed inappropriate, such website must be reported to CEO. After review of the site, appropriate steps will be taken to block inappropriate 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 CEO.

In making decisions to disable the Charter School's Technology Protection Measure device, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the Charter School. If a student claims he/she is being denied access, he/she must notify the teacher, who must submit a IT ticket requesting that the IT Department review the website to ensure that the website does not violate requirements set forth in CIPA. If the request is for a video game, the IT Department will deny the request unless the game has a legitimate educational purpose or otherwise befits the Charter School. If a question arises as to the legitimacy of the website the IT Department must consult with the Principal, who will make the final determination.

The Technology Protection Measures will be used to protect against access to visual depictions that are Obscene, harmful to Minors, illegal, pornographic, and Child Pornographic, as required by law.

Technology Protection Measures are not foolproof, and the Charter School does not warrant the effectiveness of Internet filtering except to the extent expressly required by federal and state laws. Evasion or disabling, or attempting to evade or disable, a Technology Protection Measure device installed by the Charter School is prohibited.

The Charter School shall not be held responsible when a student or other User knowingly or willingly accesses inappropriate material or communicates or shares such materials with others.

Viruses

Viruses can cause substantial damage to Technology Resources. Users are responsible for taking reasonable precautions to ensure they do not introduce viruses to the Charter School's Technology Resources.

All material received on disk, flash drive, or other magnetic or optical medium, and all materials downloaded from the Internet or from Technology Resources or networks that do not belong to the Charter School must be scanned for viruses and other destructive programs before being transferred to Charter School's Technology Resources. Any User receiving an e-mail from a questionable source must contact the IT Department before opening the e-mail or any attachment included in the e-mail.

To ensure security and avoid the spread of viruses, Users accessing the Internet through a Technology Resources attached to the Charter School's network must do so through an approved Internet firewall or Technology Protection Measure.

Encryption Software

Users shall not install or use encryption software on any Charter School Technology Resource without first obtaining written permission from the CEO. Users shall not use passwords or encryption keys that are unknown to the CEO.

The federal government has imposed restrictions on export of programs or files containing encryption technology. Software containing encryption technology shall not be placed on the Internet or transmitted in any way outside the United States.

Web Content Developed By Students

As part of class/course assignments, students may be developing and/or publishing content to the Internet via web pages, electronic and digital images, blogs, wikis, podcasts, vodcasts, and webcasts, or may be participating in videoconferences.

The following guidelines must be adhered to when students develop and publish information to the Internet:

1. Personal information such as phone numbers, addresses, e-mail addresses or other specific personal information shall not be published or shared to a public page or videoconference.
2. All web content must comply with this policy.
3. All web content and videoconferencing must be under the direction and supervision of the teacher/administrator and is to be used for educational purposes only.
4. All web content is subject to copyright law and fair use guidelines.
5. All web content shall only be posted to Charter School approved web pages, blogs, wikis, podcasts, webcasts, vodcasts and videoconferences.

Prohibitions

Students, staff and all Users are expected to act in a responsible, ethical and legal manner in accordance with Charter School policies and federal and state laws. Specifically, the following uses of the Charter School's Technology Resources are prohibited:

1. To facilitate illegal activity, including unauthorized access and hacking;
2. To engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or otherwise authorized;
3. Non-work or non-school related work;
4. Product advertisement or political lobbying;
5. Production or distribution of hate mail, unlawfully discriminatory remarks, and offensive or inflammatory communication;
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials;
7. To access or transmit material that is harmful to Minors and/or Users, indecent, Obscene, pornographic, Child Pornographic, terroristic, or advocates the destruction of property;
8. Use of inappropriate language or profanity;
9. To transmit material likely to be offensive or objectionable to recipients;
10. To intentionally obtain or modify files, data and passwords belonging to other Users, or integral to system and network operations;
11. Impersonation of another User, anonymity and/or use of pseudonyms;
12. Loading or use of unauthorized games, programs, files, or other electronic media;
13. To disrupt the work of other Users;
14. Destruction, modification, or abuse of Technology Resources and peripheral hardware or software;
15. Relocation of Charter School hardware without prior administrative consent;
16. Quoting personal communications in a public forum without the original author's prior consent;
17. To access or use any form of electronic mail on Charter School Technology Resources unless authorized by the CEO or his/her designee;
18. Using the network to participate in online or real-time conversations unless authorized by the teacher/administrator for the purpose of communicating with other classes, students, teachers, experts or professionals for educational purposes;
19. Using a disk, removable storage device or CD/DVD brought into the Charter School from an outside source that has not been properly scanned for viruses or authorized for use by a teacher/administrator in accordance with Charter School established procedures;
20. To discriminate against, advocate violence against, harass, intimidate, bully or cyberbully others;
21. To send unsolicited ("spamming") or forwarded e-mails and chain letters to persons;

22. Using "spoofing" or other means to disguise User identities in sending e-mail or other electronic communication via bulletin boards, newsgroups, social networking sites, instant messages, e-mail systems, chat groups, chat rooms, or through other Technology Resources;

23. To send, transmit or otherwise disseminate proprietary data, trade secrets, or other confidential information of the Charter School;

24. Posting or allow the posting of personal information about themselves or other people on the Technology Resources unless authorized by the CEO. Personal information includes address, telephone number (including home, work and cell phone numbers), school address, work address, pictures or video bites, clips, etc.;

25. To refer to or attempt to refer to the Charter School or its employees, agents, trustees, parents or students in any electronic communication, posting, blog, website, e-mail or social networking site, without written authorization of the CEO;

26. To access or transmit gambling, pools for money, or any other betting or games of chance;

27. To solicit information with the intent of using such information to cause personal harm or bodily injury to another or others;

28. Posting, sharing or attempting to post information that could endanger an individual, cause personal damage or a danger of service disruption; and

29. Indirectly or directly making connections that create "backdoors" to the Charter School, other organizations, community groups, etc. that allow unauthorized access to the Technology Resources or the Charter School.

30. Any conduct that is contrary to the requirements set forth in the Family/Student Handbook, Employee Handbook or any other Charter School related Policies and Procedures.

Security

The Charter School intends to strictly protect its Technology Resources against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these assets and in lessening the risks that can harm Technology Resources. Therefore, Users are required to comply fully with this Policy and to immediately report any violations or suspicious activities to the CEO.

System security is protected in part by the use of passwords. All passwords must be at least eight (8) characters and include alphanumeric and special characters. After three (5) unsuccessful access attempts, an attempted User will be locked out and must contact the CEO or his/her designee.

Failure to adequately protect or update passwords could result in unauthorized access to personal or Charter School files. Users shall be responsible for safeguarding their passwords for access to the Charter School's Technology Resources and for all transactions made using their passwords. To protect the integrity of the Charter School's Technology Resources and systems, the following guidelines shall be enforced:

1. Students and other Users shall not reveal their passwords to another unauthorized individual.

2. Passwords shall not be printed or stored online.
3. Students and other Users are required to log off from the network when they complete working at a particular station.
4. Users are not to use a computer that has been logged in under another student's, teacher's or User's name.
5. Any User identified by the CEO or his/her designee as having a history of discipline problems involving Technology Resources may be denied access to any or all of the Charter School's Technology Resources.
6. Students and other Users shall not alter a communication originally received from another person or computer with the intent to deceive.
7. Users shall not misrepresent the identity of a sender or source of communication.
8. Users shall not disable or circumvent any Charter School security; software or hardware.
9. Users shall not interfere with or disrupt the Charter School's systems, network accounts, services or equipment.
10. Files, system security software/hardware or any Charter School system shall not be altered or attempt to be altered without the written authorization of the CEO or his/her designee.
11. Unauthorized hardware and electronic devices shall not be connected to the Charter School system.
12. Users shall comply with requests from the CEO or his/her designee to discontinue activities that threaten the operation or integrity of the Charter School system.

Use of passwords to gain access to Technology Resources 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 Technology Resources. The Charter School retains access to all material stored on the Technology Resources regardless of whether that material has been encoded with a particular User's password, subject to limitations as set forth in the Charter School's policy governing Remote Access and Monitoring of the Charter School's Technology Resources as well as applicable law.

Users shall 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 shall not use the Technology Resources to "snoop" or pry into the affairs of other Users by unnecessarily reviewing the files and e-mails of another.

A User's ability to connect to another computer's system through the network or by any other electronic means shall 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 and the CEO.

Students Using Approved Personal Technology For Classroom Use

The Charter School retains the right to determine where and when personal technology may access the Charter School network. The CEO or designees will determine if Users are permitted to connect on a space-available basis and Charter School resources will receive priority over non-Charter School equipment and may connect on a space-available basis and Charter School resources will receive priority

over non-Charter School equipment. Peripheral devices such as printers may not be disconnected from the network and connected to personal technology.

All personal technology must be running up-to-date, with Charter School-approved virus detection software and operating system critical updates prior to accessing the Charter School network. Equipment must be certified as virus-free before being connected to the network.

Charter School-owned software may not be installed on personal technology without written permission from the CEO or his/her designee.

File storage on the network is limited to schoolwork only.

The Students must supply all necessary hardware and software in order to be permitted to use personal technology in the classroom.

The CEO or his/her designee has the right to deny the connection of personal technology to the network. Personal technology may be removed from the Charter School network at any time on the recommendation of the CEO or his/her designee.

Photos, digital images, videos, and recordings taken of Charter School students and staff without their consent or knowledge will not be tolerated. Violators will be subject to disciplinary actions including but not limited to loss of privileges to possess and use electronic devices on Charter School property, at Charter school sponsored events/activities and on Charter School transportation.

Personal technology discovered on the Charter School network without authorization from the CEO and/or his/her designee shall be confiscated.

Safety

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 shall immediately bring them to the attention of a teacher, staff member or an administrator.

Communications through Charter School Technology Resources are limited to only that which serves a demonstrable educational purpose. For safety reasons, Charter School Users shall not reveal personal addresses or telephone numbers to other Users on Charter School networks or on the Internet.

The CEO or his/her designee shall be responsible for implementing protection measures to determine whether Charter School's computers, laptops, iPads, Kindles and other Technology Resources and technology related devices such as USB drives, digital cameras and video cameras, PDAs, MP3 players, printers, etc. are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing technology protection measures that block or filter Internet access for minors and adults to certain visual depictions that are Obscene, Child Pornography, harmful to minors with respect to use by Minors, or determined inappropriate for use by Minors by the Board of Trustees.

2. Approved employees and/or vendors with access to the room that contains Charter School's server.
3. Removing terminated employees and vendors from the Charter School's system in a timely manner.
4. Analyzing the impact of proposed program changes in relation to other critical business functions before adopting the proposed program changes.
5. Developing compensating controls to mitigate information technology (IT) weakness to student data, i.e. reconciliations to manual records, analysis of student trends, data entry procedures and review, etc.

Vendors

If the Charter School shares internally sensitive or legally/contractually restricted Charter School data with parties outside the Charter School community, the Charter School shall first enter into a Non-Disclosure Agreement with the party. The Non-Disclosure Agreement is needed to protect the Charter School's proprietary or otherwise sensitive information. Non-Disclosure Agreements are typically needed when entering into a business relationship with vendors, consultants and contractors. All Non-Disclosure Agreements must be reviewed by the Charter School's legal counsel before signing.

All vendors, consultants and/or contractors shall only be granted access to the Charter School's Technology Resources to make changes or updates with prior written authorization from the CEO or his/her designee. Once the vendor, consultant and/or contractor, completes its work, access to the Charter School's Technology Resources will be removed.

Vendors, consultants and contractors are required to assign unique user IDs and passwords to each of their employees authorized to access the Charter School's system. Vendors, consultants and/or contractors may be terminated for violating this Policy and/or violating any state or federal laws.

All vendors, consultants and/or contractors and their employees who have direct contact with students must comply with the mandatory background check requirements for federal and state criminal history and child abuse. An official child abuse clearance statement for each of the vendors', consultants' and/or contractors' employees shall be submitted to the Charter School prior to beginning employment with the Charter School. Failure to comply with the background check requirements shall lead to immediate termination.

Closed Forum

The Charter School's Technology Resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.

All expressive activities involving Charter School Technology Resources that students, parents/guardians and members of the public might reasonably perceive to bear the approval of the Charter School and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the Charter School for legitimate educational reasons. All other expressive activities involving the Charter School's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board of Trustees policies.

Records Retention

Charter School personnel shall establish a retention schedule for the regular archiving or deletion of data stored on Charter School Technology Resources that complies with the Charter School's Record Retention and Destruction Policy as well as all federal and state laws and regulations. It is the User's responsibility to know which records are subject to these conditions and to comply with these laws and regulations or to contact the CEO for clarification.

In the case of pending or threatened litigation, the Charter School's attorney will issue a litigation hold directive to the CEO or his/her designee. A hold directive will direct all Charter School administration and staff not to delete or destroy any electronic mail or other documentation on a computer as related to a specific student, employee, issue and/or for a specific time period. Failure to follow such a directive could result in negative legal consequences for the User and/or within the actual or threatened litigation. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the Charter School's attorney.

E-mail and computer accounts of separated employees that have been placed on a litigation hold will be maintained by the Charter School until the hold is released. No employee, who has been so notified of a litigation hold, may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Drafting E-mails

Like any other document, an e-mail message and other computer information is discoverable during litigation. An e-mail may be used in litigation to indicate what a User knew or felt. It is important to keep this in mind when creating e-mails 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. Since e-mail communications are discoverable during litigation, they will have to be turned over to the opposing party unless determined to be privileged by the Charter School's legal counsel.

Privileged Attorney-Client Communications

Confidential e-mail sent to or retained from counsel or an attorney representing the Charter School shall include this warning header on each page: "ATTORNEY CLIENT PRIVILEGED: DO NOT FORWARD WITHOUT PERMISSION" or some other similar warning header that communicates the privileged nature of the communication.

Damages

All damages incurred by the Charter School due to a User's intentional or negligent misuse of Charter School's Technology Resources, including loss of property and staff time, may be charged to the User. Charter School administrators have the authority to sign any criminal complaint regarding damage to Charter School technology.

No Warranty/No Endorsement

The Charter School makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides.

The electronic information available to students and staff on the Internet or through web-based services does not imply endorsement of the content by the Charter School, with the exception of resources approved and adopted by the Board of Trustees. Nor does the Charter School guarantee the accuracy of information received using the Charter School's Technology Resources.

The Charter School is not and shall not be responsible for the loss of data, delays, non-deliveries, miss-deliveries or service interruptions. The Charter School is not and shall not be responsible for any information that may be damaged or unavailable when using Charter School Technology Resources or for any information that is retrieved via the Internet. The Charter School is not and shall not be responsible for any damages incurred as the result of using the Charter School's Technology Resources, including but not limited to, the loss of personal property used to access Technology Resources. Further, the Charter School is not and shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other commercial online services.

Unauthorized Disclosure of Information of Minors

It is a violation of state laws, including, but not limited to Chapter 12 of Title 22 of the Pennsylvania Code, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g)[9] and all other federal laws and regulations, to access data of a student the User does not have a legitimate educational interest in or to disclosure information about a student without parental permission or absent an exception to the disclosure requirements. 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 Charter School's student records and confidentiality policies. Unauthorized disclosure, use and dissemination of personal information regarding Minors is prohibited.

Compliance with Applicable Laws and Licenses

In their use of Technology Resources, Users must comply with all software licenses/copyrights and all other state, federal, and international laws governing intellectual property and online activities. Users shall 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 it is confirmed in advance from appropriate sources that the Charter School has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the Charter School, as well as legal action by the copyright owner. Any questions concerning these rights should be directed to the CEO or his/her designee.

Violations of Acceptable Technology Usage Policies and Procedures

Use of Technology Resources and equipment in a disruptive, manifestly inappropriate or illegal manner impairs the Charter School's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all Users granted access to the Charter School's Technology Resources. Any violation of Charter School policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of User privileges. User privileges may be suspended pending investigation into the use of the Charter School's Technology Resources and equipment.

Employees may be disciplined or terminated, and students suspended or expelled, for violating this Policy. Any attempted violation of the Charter School's policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Consequences for Inappropriate Use

Charter School Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of Charter School Technology Resources includes, but is not limited to: intentional copying, deletion or damage to files or data belonging to others, copyright violations, or theft of services. Any illegal usage of Charter School Technology Resources will be immediately reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet or any Charter School Technology Resource. Suspension of access, loss of access and other disciplinary actions may be consequences for inappropriate use. Vandalism may result in cancellation of access privileges, discipline and possible criminal action.

Cessation of Access

Upon termination or ending of enrollment, employment or the termination of any contract with or from the Charter School, no further access to or use of Technology Resources is permitted without the express authorization from the CEO.

Education of Technology Resource Users

The Charter School shall implement a program that educates students and staff about acceptable use and internet safety associated with the Charter School's Technology Resources. All students must complete a designated Technology Resources and Internet training prior to unsupervised use of the Charter School's Technology Resources as required by the 2008 Broadband Data Improvement Act. This training includes, but is not limited to: appropriate online behavior, including interacting on social networking websites and in chat rooms; cyberbullying awareness and response; proper use of Technology Resources; restricted activities with Technology Resources; and access and monitoring of school-issued Technology Resources to students.

No Additional Rights

This Policy is not intended for and does not grant Users any contractual rights.

Users of the Charter School's Technology Resources must review this policy closely and sign and return to Charter School a form acknowledging receipt and acceptance of the terms in this policy, which is attached hereto. Venue for any legal action arising out of an alleged and/or actual violation of the attached Agreement(s) shall be in Montgomery County, Pennsylvania.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH THE SCHOOL'S CHARTER OR APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS AND/OR CHARTER CONTROL.

Legal References:

1. 47 U.S.C. §§ 254(h) and (l)[1]
2. Neighborhood Children's Internet Protection Act (NCIPA)
3. 2008 Broadband Improvement Act, P.L. 110-385
4. 18 U.S.C.A. §2256(8)
5. 18 PA CSA §6312(d)
6. Miller v. California, 413 U.S. 15 (1973)
7. 18 U.S.C. § 2246(2)
8. 18 Pa.C.S.A. § 5903
9. 20 U.S.C. § 1232g

Acknowledgement of the Acceptable Use and Internet Safety Policy (Student User Agreement)

Dear Parent/Guardian:

Please review the following Student User Agreement with your child. Then please return both the signed Student User Agreement and the signed Parent User Agreement, which acknowledges receipt of **Chester Community Charter School's** ("Charter School") Acceptable Use and Internet Safety Policy ("Policy"), to your child's principal by **{_____}**. This form is valid for the duration of your child's enrollment in Charter School until replaced by another form or revoked in writing by a parent or guardian.

I, _____, a student of Charter School, have read the entire Policy understand it and agree to comply with the Policy. In addition to complying with all terms of the Policy, when using any Charter School Technology Resources, as defined above, I accept the following basic rules:

I shall treat all Technology Resources with care and will leave them in good working condition when I am finished. I will not damage, deface, destroy or render inaccessible Technology Resources.

I shall use appropriate language on all Technology Resources. If the language is obscene, vulgar, defamatory, harassing, degrading, sexually explicit, threatening, violent, insulting, demeaning, harmful to minors, child pornographic, pornographic, advocating illegal acts, or otherwise inappropriate as deemed by the Chief Executive Officer of the Charter School (CEO), I will not access it, use it, send it, share it, create it or attempt to access, use, create, share or send it.

I shall always treat people online with respect. I shall not use any Charter School Technology Resources to insult, harass, threaten, bully or cyberbully other Users, as defined above. I assume responsibility for the content of messages I send to others or that are sent to others via my account.

I shall respect the privacy of other Users and will not make any attempts to gain access into the private

mailboxes or accounts of those Users. I shall not allow other Users access to my mailbox and will keep my password private.

I understand that Technology Resources are to be used for educational/professional/contractual use.

I understand that all Technology Resources belong to Charter School and I shall treat them with respect.

I will not install or download any applications (games), programs or materials from the Internet or from any Technology Resources unless the CEO gives me prior permission in writing.

I shall not add any software to Charter School's Technology Resources unless the CEO gives me prior permission in writing.

I understand that the Technology Resources provided to me for use may be protected under copyright law. I agree not to copy resources unlawfully and/or distribute any materials provided for my use without express prior permission by the CEO.

I shall comply with all applicable state and federal laws and regulations regarding the use of Technology Resources, including but not limited to laws regarding child welfare and the Internet protection of minors, such as CIPA and N-CIPA.

By signing below, I agree to abide by the Policy and understand that failure to follow all rules as explained in this document may result in the loss of my privileges to Technology Resources; disciplinary action, including student disciplinary action up to and including expulsion from Charter School in accordance with the Code of Conduct; charges for damages; and civil or criminal penalties.

X

_____

(User Signature) **(Date)**

(MAINTAIN ONE COPY AND RETURN ONE COPY TO CHARTER SCHOOL)