



Book	Policy Manual
Section	6000 Operations
Title	Acceptable Use and Internet Safety
Code	6015
Status	Active
Adopted	September 13, 2016
Last Revised	May 11, 2021
Prior Revised Dates	January 15, 2019

### **Purpose**

The Board of Trustees of the 21st Century Cyber Charter School (21CCCS) provides computer network and technology resources to enhance educational opportunities for 21CCCS students, employees, and the 21CCCS community. This policy details acceptable use of technology resources provided by 21CCCS. These services and equipment are provided by 21CCCS as a privilege to the user, and appropriate and ethical use of any 21CCCS technology resources, tools, and equipment is required.

It is every technology resource user's (see "Definitions" below) 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 the acceptable use of technology resources by both adults and minors.

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) and the Neighborhood Children's Internet Protection Act (N-CIPA), the 2008 Broadband Improvement Act, P.L. 110-385, and any applicable implementing regulations. As such, this policy addresses the following: [\[1\]](#)[\[2\]](#)[\[3\]](#)[\[4\]](#)

1. Access by minors to inappropriate matter on the Internet and World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including so-called hacking and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

In using or accessing 21CCCS' technology resources, users must comply with the provisions outlined in this policy.

### **Definitions**

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

Technology resources means technologies, devices, and resources used to access, store, or communicate information. This definition includes, but is not limited to: computers, information systems, networks, laptops, iPads or other tablet devices, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audiovisual equipment, digital cameras, e-readers (i.e. Kindles and Nooks), Internet, electronic mail, electronic communications devices and services, multimedia resources, hardware, and software, including Moodle software.

User means any person who has signed this policy and is permitted by 21CCCS to utilize any portion of 21CCCS' technology resources, including, but not limited to, students, parents/guardians, Learning Coaches, employees, Board of Trustees members, contractors, consultants, vendors, and agents of 21CCCS.

User identification (User ID) means any identifier that would allow a user access to 21CCCS's technology resources or to any program including, but not limited to, email and Internet access.

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

Child Pornography means, under federal law, any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where:[\[5\]](#)

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.

Under Pennsylvania law, child pornography is 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.[\[6\]](#)

Minor means, for purposes of compliance with CIPA, an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean any person under the age of eighteen (18).

Obscene means, under federal and Pennsylvania law, any material if:[\[7\]](#)

1. The average person, applying contemporary 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.

Technology protection measure means a specific technology that blocks or filters Internet access to content that is obscene, child pornography, or harmful to minors and the material covered by a certification regarding CIPA.[\[3\]](#)

Sexual act and sexual contact have the meanings given such terms under 18 U.S.C. § 2246(2), 18 U.S.C. § 2246(3), and 18 Pa.C.S.A. § 5903.[\[7\]](#)[\[8\]](#)

Vandalism means any malicious attempt to harm or destroy technology resources or data of another user, on the Internet, or on other networks. This includes, but is not limited to, the uploading or creation of computer viruses or malware.

## **Guidelines**

### **Authorized Users**

21CCCS's technology resources may be used by any authorized user. Use of 21CCCS's technology resources is a privilege, not a right. If a potential user has a history of discipline problems involving technology resources, the Chief Executive Officer (CEO) or designee may make the decision not to give the potential user access to certain 21CCCS technology resources.

### **User Privacy**

Computer accounts and technology resources are given to users to assist them in the performance of 21CCCS-related functions. A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving 21CCCS' technology resources, including email, in anything they create, store, send, share, access, view, or receive on or through the Internet.

By using 21CCCS' 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 21CCCS in accordance with 21CCCS policies and procedures. A user ID with email access will be provided to authorized users only on the conditions that the user consent to interception of or access to all communications accessed, sent, received, or stored using 21CCCS technology and sign this policy.

Electronic communications, downloaded material, and all data stored on 21CCCS' technology resources, including files deleted from a user's account, may be intercepted, accessed, or searched by 21CCCS administrators or designees at any time in the regular course of business to protect users and 21CCCS' 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 of Trustees directs the CEO or designee to assign trained personnel to maintain 21CCCS's technology in a manner that will protect 21CCCS from liability and will protect confidential student and employee information retained on or accessible through 21CCCS' technology resources.

Administrators may suspend access to and/or availability of 21CCCS' technology resources to diagnose and investigate network problems or potential violations of the law or 21CCCS policies and procedures. All 21CCCS technology resources are considered 21CCCS property.

21CCCS may maintain or improve technology resources at any time. 21CCCS or authorized 21CCCS 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**

School computers will be outfitted with software to enable school officials to remotely monitor and administer the computer. 21CCCS shall not remotely access any webcam or video camera on any computer or electronic device issued to a student without obtaining prior written permission from the parents/guardians (or student if age 18 or older). 21CCCS issued devices are configured with a content filter enabled to block inappropriate content in accordance with the Children's Internet Protection Act (CIPA). In addition, all devices are under enrollment in a mobile device management (MDM) service. This service is used to install software, apply updates, and provide additional device restrictions. It is a violation of school rules and school board policies to circumvent these services.

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 an inappropriate site from users.[\[1\]](#)[\[3\]](#)[\[9\]](#)

For purposes of bona fide research or other lawful purposes, certain blocked sites may be made available—but only after approval by the CEO. In making decisions to disable 21CCCS' Technology Protection Measure device, the CEO or designee shall consider whether the use will serve a legitimate educational purpose or otherwise benefit 21CCCS. A student or parent/guardian claiming they have been denied access to Internet material that is not within the purview of this policy shall be afforded review of the request. The parent/guardian or student (if age eighteen (18) or older) must notify the CEO or designee electronically or in writing that they are requesting a reconsideration review within ten (10) school days. Once a decision is rendered, if the parent/guardian or student disagrees with the decision, the parent/guardian or student may escalate their request to the 21CCCS Board of Trustees.[\[1\]](#)[\[9\]](#)[\[10\]](#)

Technology Protection Measures are not foolproof, and 21CCCS 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 21CCCS is prohibited.

21CCCS 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 21CCCS' 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 21CCCS, must be scanned for viruses and other destructive programs before being transferred to 21CCCS' systems. Any user receiving an email from a questionable source must contact the Technology Department before opening the email or any attachment included in the email.

To ensure security and avoid the spread of viruses, users accessing the Internet through a technology resource attached to 21CCCS' 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 21CCCS 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, and/or may be participating in videoconferences.

1. Personal information such as phone numbers, addresses, email 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 Learning Coach 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 be posted only to 21CCCS–approved Web pages, blogs, wikis, podcasts, webcasts, vodcasts, and/or videoconferences.

### **Prohibitions**

Students, staff, and all users are expected to act in a responsible, ethical, and legal manner in accordance with 21CCCS policies and federal and state laws. Specifically, the following uses of 21CCCS' technology resources are prohibited:

1. To facilitate illegal activity, including unauthorized access and hacking.
2. Evasion or disabling, or attempting to evade or disable, a Technology Protection Measure device installed by 21CCCS.
3. To engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or otherwise authorized.
4. Non-work or non-school-related work.
5. Product advertisement or political lobbying.
6. Production or distribution of hate mail, unlawful discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. To access or transmit material that is harmful to minors and/or users, indecent, obscene, pornographic, child pornographic, or terroristic, or that advocates the destruction of property.
9. Use of inappropriate language or profanity.
10. To transmit material likely to be offensive or objectionable to recipients.
11. To intentionally obtain or modify files, data, and passwords belonging to other users or integral to system and network operations.
12. Impersonation of another user, anonymity, and/or use of pseudonyms.
13. Installing or use of unauthorized games, programs, files, or other electronic media.
14. To disrupt the work of other users.
15. Destruction, modification, or abuse of technology resources and peripheral hardware or software.
16. Relocation of 21CCCS hardware without prior administrative consent.
17. Quoting personal and/or private communications in a public forum without the original author's prior consent.
18. To access or use any form of non-21CCCS electronic mail on 21CCCS technology resources unless authorized by the CEO or designee.

19. 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 and/or professionals for educational purposes.
20. Using a disk, removable storage device, or CD/DVD, brought into 21CCCS from an outside source, that has not been properly scanned for viruses or authorized for use by a teacher/administrator in accordance with 21CCCS established procedures.
21. To discriminate against, advocate violence against, harass, intimidate, bully, or cyberbully others.
22. To send unsolicited or forwarded emails and chain letters to persons ("spamming").
23. Using "spoofing" or other means to disguise user identities in sending email or other electronic communication via bulletin boards, newsgroups, social networking sites, instant messages, email systems, chat groups, chat rooms, or other technology resources.
24. To send, transmit, or otherwise disseminate proprietary data, trade secrets, or other confidential information of 21CCCS.
25. To post or allow the posting of personal information about oneself or other people on the technology resource unless authorized in advance 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 and so forth.
26. To refer to or attempt to refer to 21CCCS or its employees, agents, trustees, parents/guardians, or students in any electronic communication, posting, blog, website, email, or social networking site, without written authorization from the CEO.
27. To access or transmit gambling, pools for money, or any other betting or games of chance.
28. Using technology resources to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others.
29. Using technology resources to post, share, or attempt to post or share information that could endanger an individual or cause personal damage or a danger of service disruption.
30. Indirectly or directly making connections that create "back doors" to 21CCCS, other organizations, community groups, etc., that allow unauthorized access to the technology resources or 21CCCS.
31. Use of school-issued devices or 21CCCS internet resources or accounts outside of the United States of America without the prior written consent of the CEO.

### **Security**

21CCCS 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.

Employee users will be required to change their passwords every thirty (30) days.

Student users will be required to change their passwords every six (6) months.

21CCCS will maintain a password history that prevents the use of a repetitive password.

After three (3) unsuccessful access attempts, an attempted user will be locked out and must contact the Help Desk.

After a period of 60 (sixty) minutes of inactivity, a user will be automatically logged off the system.

In addition, there may be circumstances that warrant the change of a password, including but not limited to the following:

1. The user's laptop has been replaced with a new unit;
2. There has been a record or report of a virus or other potentially dangerous software or malware on the user's system;

3. The user's system has been compromised by hacking or there is a reasonable suspicion of such activity;
4. The user has admitted to sharing a password, or there are reasons to believe that a user's password has been shared, with another student or other non-authorized user; or
5. Other reasons determined by the 21CCCS Technology Department.

Failure to adequately protect or update passwords could result in unauthorized access to personal or 21CCCS files. Users shall be responsible for safeguarding their passwords for access to 21CCCS's technology resources and for all transactions made using their passwords. To protect the integrity of 21CCCS 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 finish 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 designee as having a history of discipline problems involving technology resources may be denied access to any or all of 21CCCS' 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 21CCCS security, software or hardware.
9. Users shall not interfere with or disrupt 21CCCS' systems, network accounts, services, or equipment.
10. Files, system security software/hardware, or any 21CCCS system shall not be altered or attempt to be altered without the written authorization of the CEO or designee.
11. Unauthorized hardware and electronic devices shall not be connected to the 21CCCS system.
12. Users shall comply with requests from the CEO or designee to discontinue activities that threaten the operation or integrity of the 21CCCS 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. 21CCCS retains the right to access 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 21CCCS' Remote Access and Monitoring of School-Issued Technology Policy 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 emails 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 make use of those systems unless specifically authorized by the administrators of those systems and the CEO. Users shall not use the technology resources to snoop or pry into the affairs of other users by unnecessarily or inappropriately reviewing the files and/or emails of another.

## **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 administrator.

Communications through 21CCCS technology resources are limited to only those which serve a demonstrable educational purpose. For safety reasons, 21CCCS users shall not reveal personal addresses, contact information or telephone numbers to other users on 21CCCS networks or on the Internet.

The CEO or designee shall be responsible for implementing protection measures to determine whether 21CCCS' computers, laptops, iPads, Kindles, tablets 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:[\[1\]](#)[\[2\]](#)[\[3\]](#)

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. Maintaining a listing of all employees and users with access to the room which contains 21CCCS' server.
3. Generating and maintaining monitoring reports (including firewall logs) of user activity and remote access on 21CCCS' system by all users, including but not limited to students, employees, contractors, consultants, and/or vendors.
  - a. The report should include the date, time, and reason for access; whether it was remote access; the changes made; and who made the changes.
4. Maintaining documentation that students no longer enrolled at 21CCCS as well as terminated employees and contractors/vendors or those with expired contracts have been properly removed from 21CCCS' system in a timely manner.
5. Analyzing the impact of proposed program changes in relation to other critical business functions before adopting the proposed program changes.
6. Developing compensating controls to mitigate IT weakness and alert 21CCCS to unauthorized changes to student data, i.e., reconciliations to manual records, analysis of student trends, data entry procedures and review, etc.

### **Vendors**

If 21CCCS shares internally sensitive, legally-and/or contractually-restricted 21CCCS data with parties outside the 21CCCS community, 21CCCS shall first enter into a Non-Disclosure Agreement with the party. The Non-Disclosure Agreement is needed to protect 21CCCS' 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 21CCCS' legal counsel before signing.

All vendors, consultants, and/or contractors shall be granted access to 21CCCS' technology resources only to make changes or updates with prior written authorization from the CEO or designee. Once the vendor, consultant, and/or contractor have completed their work, access to 21CCCS' systems will be removed.

Vendors, consultants, and contractors are required to assign unique user IDs and passwords to each of their employees authorized to access 21CCCS' 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 Pennsylvania 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 21CCCS prior to beginning employment with 21CCCS. Failure to comply with the background checks as required by applicable law or legal regulations and/or the Pennsylvania Department of Education shall lead to immediate termination or non-hire.[\[11\]](#)[\[12\]](#)[\[13\]](#)

### **Closed Forum**

21CCCS' 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 21CCCS technology resources that students, parents/guardians, and members of the public might reasonably perceive to bear the approval of 21CCCS 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, to the fullest extent permitted by applicable law, on behalf of 21CCCS for legitimate educational reasons. All other expressive activities involving 21CCCS's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by applicable law and Board of Trustees Policies.

### **Records Retention**

21CCCS personnel shall establish a retention schedule for the regular archiving or deletion of data stored on 21CCCS technology resources that complies with 21CCCS' Record Retention and Destruction Policy as well as all federal and Pennsylvania 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, 21CCCS' attorney will issue a litigation hold directive to the CEO or designee. A hold directive will direct all 21CCCS administration and staff or agents not to delete or destroy any electronic mail or other documentation on a computer as related to a specific student, employee, and issue 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 21CCCS' attorney.

Email and computer accounts of separated employees that have been placed on a litigation hold will be maintained by 21CCCS 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 Emails**

Emails may appear informal, as email messages are sometimes offhand like a conversation and are often not as carefully thought out as a letter or memorandum. Like any other document, an email 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 email messages and other documents. Even after you delete an email message or close a computer session, it may still be recoverable and may remain on the system. Email communications are discoverable during litigation and, therefore, will have to be turned over to the opposing party unless it is determined to be privileged by 21CCCS' legal counsel.

### **Privileged Attorney-Client Communications**

Confidential emails sent to or retained from counsel or an attorney representing 21CCCS shall include this warning header on each page: "ATTORNEY CLIENT PRIVILEGED" and/or "ATTORNEY CLIENT PRIVILEGED: DO NOT FORWARD WITHOUT PERMISSION."

### **No Warranty/No Endorsement**

21CCCS 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 21CCCS, with the exception of resources approved and adopted by the Board of Trustees. Nor does 21CCCS guarantee the accuracy of information received using 21CCCS' technology resources.

21CCCS is not and shall not be responsible for the loss of data, delays, nondeliveries, misdeliveries, or service interruptions. 21CCCS is not and shall not be responsible for any information that may be damaged or unavailable when using 21CCCS technology resources or for any information that is retrieved via the Internet. 21CCCS is not and shall not be responsible for any damages incurred as the result of using 21CCCS technology resources, including but not limited to the loss of personal property used to access a technology resource. Further, 21CCCS 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, as well as The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) 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 disclose information about a student without parental permission or absent an exception to the disclosure requirements. Access and distribution of student data is recorded.[\[14\]](#)[\[15\]](#)

Questions regarding the disclosure of student information must be directed to the CEO prior to disclosure and must conform to 21CCCS' Student Records Policy. Unauthorized disclosure, use, and/or dissemination of personal information regarding minors is prohibited.

### **Damages**

Users shall be responsible for damage to technology resources, equipment, systems, and/or software. All damage incurred due to a user's intentional or negligent misuse of 21CCCS' technology resources, including loss of property and staff time, may be charged to the user. 21CCCS administrators have the authority to sign any criminal complaint regarding damage to 21CCCS technology.

### **Technology Optional Insurance**

The technology devices provided by 21st Century Cyber Charter School are expensive devices that require students to follow usage guidelines and use caution when handling the devices. All students are assigned a MacBook Air and an iPad. A charger is also provided for each device. It is the student's responsibility to care for the devices and any accessories. **The technology optional insurance is highly recommended, but not required.** The annual fee covers the cost of repairing devices. Fees are capped at a maximum of two fees per household. The optional insurance cost for the current school year is as follows:

Per Student Cost	Per Student Cost Qualifies for Reduced Lunch Status	Per Student Cost Qualifies for Free Lunch Status	Per Student Cost Opt Out
\$25	\$10	\$0	\$0

If the MacBook Air or iPad is stolen or lost, including as a result of fire or other natural disaster, you must notify the school immediately and file a police report for stolen devices. It is highly recommended to add the devices to your homeowners or renters insurance policy. The student will be responsible for the cost of stolen or lost devices at the respective fee:

MacBook Air	\$699.00
MacBook Air Charger	\$72.00
iPad	\$294.00
iPad Charger	\$19.00
iPad Lightning Cable	\$19.00

Should there be any damage to the devices, it must be reported within 24 hours and the Technology Department will determine if the damage was deliberate or as a result of deterioration from use. Any damage caused deliberately will be classified as vandalism. Students will be billed for repairs caused by vandalism and disciplinary action may occur. The optional insurance covers the first incident of the school year, including damage due to negligence or vandalism. Subsequent incidents will incur a deductible based on the tier of damage.

#### Important Notes:

- The optional insurance MUST be paid prior to an incident occurring. It will not be applied retroactively.
- If the damage involves multiple tiers you will be charged the highest of the tiers.
- Examples of negligence or vandalism include, but are not limited to:
  - Lying or misrepresenting information on the damage reported
  - Not reporting damages on time
  - Damage caused by drops, falls, collisions or liquid spills

The following shows deductible costs based on tier and type of damage.

Device Type	Damage Tier	Type of Damage	Subsequent Incident Cost with Tech Fee	ANY Incident Cost WITHOUT Tech Fee
MacBook Air	Tier 1	Internal Components, Cables, Connectors, etc.	No Charge	Up to \$15.00
MacBook Air	Tier 2	Trackpad	\$15.00	\$45.00
MacBook Air	Tier 2	Wireless Card	\$20.00	\$60.00
MacBook Air	Tier 2	Bottom Case	\$23.00	\$70.00

MacBook Air	Tier 3	Battery	\$33.00	\$100.00
MacBook Air	Tier 3	Top Case w/Keyboard	\$60.00	\$180.00
MacBook Air	Tier 4	SSD	\$73.00	\$220.00
MacBook Air	Tier 4	LCD Display	\$103.00	\$310.00
MacBook Air	Tier 4	Logic Board	\$103.00	\$310.00
iPad	Tier 1	Home Button	No Charge	\$5.00
iPad	Tier 1	Front/Back Camera	No Charge	\$5.00
iPad	Tier 1	Speakers	No Charge	\$5.00
iPad	Tier 1	Headphone Jack	No Charge	\$5.00
iPad	Tier 2	Digitizer	\$12.00	Up to \$35.00
iPad	Tier 2	LCD Screen	\$46.00	Up to \$140.00
iPad	Tier 2	Battery	\$6.00	\$20.00

Insurance can be purchased online via: <http://https://school.21cccs.org/mod/resource/view.php?id=49829>

Click here to register or sign in to the payment portal. Check payment may be sent to the school's attention to the Business Office. No cash will be accepted.

### **Reporting a Missing or Stolen Technology Resource**

If a student or parent/guardian believes that a school-issued technology resource is missing or stolen, the following must occur:

1. Notify the student's Family Support Coordinator immediately;
2. Immediately file a true and accurate report with the local police department and/or law enforcement agency;
3. Immediately submit a copy of the report via email, fax or US Mail to the IT Director at the 21st Century Cyber Charter School; and
4. Cooperate with 21CCCS and/or authorities in any and all legal efforts/actions taken to retrieve the stolen property.

### **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 email system or by any other means unless it is confirmed in advance from appropriate sources that 21CCCS has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by 21CCCS as well as legal action by the copyright owner. Any questions concerning these rights should be directed to the CEO or designee.<sup>[16]</sup>

### **Violations of Acceptable Technology Usage Policies and Procedures**

Use of technology resources and equipment in a disruptive, manifestly inappropriate or illegal manner impairs 21CCCS' mission and squanders resources, and it shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to 21CCCS' technology resources. Any violation of 21CCCS 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 21CCCS' technology resources and equipment.<sup>[9]</sup>

Employees may be disciplined or terminated, and students suspended or expelled, for violating this policy. Any attempted violation of 21CCCS' 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**

Illegal use of 21CCCS 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 21CCCS technology resources will be immediately reported to the appropriate legal and/or law enforcement authorities for possible investigation and prosecution.[9]

General rules for behavior and communications apply when using the Internet or any 21CCCS 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.[9]

### **Cessation of Access**

Upon the termination or ending of enrollment or employment or the termination of any contract with or from 21CCCS, no further access to or use of technology resources is permitted without the express authorization from the CEO.

### **Education of Technology Resource Users**

21CCCS shall implement a program that educates students and staff about acceptable use and Internet safety associated with 21CCCS' technology resources. All students must complete a designated technology resources and Internet training prior to unsupervised use of 21CCCS 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.[3]  
[17]

### **No Additional Rights**

This policy is not intended for and does not grant users any contractual rights. Users of 21CCCS' technology resources must review this policy closely and sign and return to 21CCCS the 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 Chester County, Pennsylvania.

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

Legal	<a href="#">1. 20 U.S.C. 6777</a>
	<a href="#">2. 47 CFR 54.520</a>
	<a href="#">3. 47 U.S.C. 254</a>
	<a href="#">4. 15 U.S.C. 6551</a>
	<a href="#">5. 18 U.S.C. 2256</a>
	<a href="#">6. 18 Pa. C.S.A. 6312</a>
	<a href="#">7. 18 Pa. C.S.A. 5903</a>
	<a href="#">8. 18 U.S.C. 2246</a>
	<a href="#">9. 24 P.S. 4604</a>
	<a href="#">10. 24 P.S. 4610</a>
	<a href="#">11. 23 Pa. C.S.A. 6344</a>
	<a href="#">12. 24 P.S. 111</a>
	<a href="#">13. 24 P.S. 111.1</a>
	<a href="#">14. 20 U.S.C. 1232g</a>
	<a href="#">15. 22 PA Code 12.31</a>

[16. 17 U.S.C. 101 et seq](#)

[17. 24 P.S. 1303.1-A](#)

[24 P.S. 1716-A](#)

[24 P.S. 1743-A](#)

[24 P.S. 4601 et seq](#)



6015-Attachments.pdf (84 KB)