THE PHOENIX CENTER

PREPARING STUDENTS FOR LIFE BEYOND THE CLASSROOM

est. 1991

Accredited by NCASES and Middle States Association

443 - ACCEPTABLE USE POLICY FOR SCHOOL TECHNOLOGY (STUDENT)

Approved by the Board of Directors on 9/10/2019

Policy

PROPER & ACCEPTABLE USE: Internet access is available to all students at The Phoenix Center (TPC). This document is the **Acceptable Use Policy** (AUP) for use at TPC. This Internet system has been established for a limited educational purpose to include classroom activities, career development, and self-discovery activities. This policy includes, but is not limited to the use of computers, Chromebooks, mobile devices, internet access, google apps for education suite, and internet applications. TPC has the right to place reasonable restrictions on the material accessed or posted, and to enforce all rules set forth in the school code and laws of the State of New Jersey. Further, this network may not be used for commercial purposes to offer, provide or purchase products or services through the system. If TPC student violates any of the provisions of the Acceptable Use Policy, his or her access privileges may be suspended or revoked, and future access privileges could possibly be denied.

INTRODUCTION: TPC offers Internet access to students during the school day. TPC provides computer equipment, computer services, and Internet access to its students for educational purposes only, offering vast, diverse, and unique resources to promote educational excellence. TPC strives to provide its students with a curriculum that is supportive, inclusive, and develops academic and life skills that boost confidence and self-esteem. Rapid advancements in technology as they relate to education offer both incredible opportunities and significant challenges. TPC will develop curriculum and apply instructional methods that will ensure our students are proficient users of emerging technologies.

The purpose of this document is to inform parents, guardians and students and all TPC users of the availability of the Internet resources, as well as the rules governing its use, and to obtain express parental or guardian permission for an individual student to use technology and the Internet while at school.

The computer system is the property of TPC, and all computer software and hardware belong to it. Therefore, TPC retains the right to monitor all access to and use of the Internet, e-mail, computers, iPads/mobile devices and network. The system is designed to keep a record of all activity on and off the Internet, and this information is also TPC property. It is important for all users to understand that no use of the Internet or e-mail can ever be guaranteed private. TPC will not be responsible for any damage you may suffer including, but not limited to, loss of data or interruptions of service. TPC is not responsible for accuracy or quality of the information attained through or stored on the system. TPC will not be responsible for financial obligations arising from unauthorized use of the system. Users are required to take full responsibility for their use of TPC Network and the Internet access.

TPC also recognizes that students have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity is included in this AUP.

Due to the complex association between many government agencies and networks, the end user (i.e. student) of these networks must adhere to strict guidelines. They are provided here so that staff, community, student users and the parents/guardians of students are aware of their responsibilities.

TPC is in compliance with the *Children's Internet Protection Act* and has installed technology protection measures for all internet-connected devices in TPC, including, but not limited to computers, tablets, Chromebooks throughout the building, that block and/or filter visual depictions that are obscene as defined in section 1460 of Title 18, United States Code; child pornography, as defined in section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image files or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political or scientific value as to minor.

Procedure

USER ACCOUNT PASSWORDS: All student passwords used on a school-provided device or with school-provided software will be created and assigned by the classroom teacher and/or the Integrative Technology Coordinator. Any student to whom an account is given is the *only* student to use that account. Each user is responsible for the security of the system. **Passwords should not be shared or written down.** If a user shares a password with another, that user is as responsible for any ensuing action as the person performing the action and will be held accountable.

THE INTERNET is an electronic highway, connecting thousands of computers all over the world, which can give students and teachers access to a variety of rich, educational resources. The World Wide Web, a portion of the Internet that students can use, includes some information specifically designed for children, up-to-the-minute scientific information, Supreme Court documents, and other information that is traditionally difficult to obtain in the school environment. To access the Internet at school, students will be using school-issued iPads, iPods, Chromebooks, or classroom computers. Information is presented richly in text, pictures, sound and video.

The educational value of appropriate information on the Internet is substantial and invaluable. The Internet is composed of information provided by institutions and people all over the world; however, also includes material that is not of educational value in the context of the school setting. There is information that may be judged as inaccurate, abusive, profane, sexually oriented or illegal. TPC does not condone or permit the use of this material and has the right to place reasonable restrictions on the material that is accessed or posted through TPC's network.

Internet access is available throughout the school building. Practicing active supervision, school personnel will, to the extent possible, always oversee student technology access.

E-MAIL: Students may be assigned an email through the Google Suite For Education (GSFE) account (thephoenixcenternj.org). The teacher and the student will have access to the school designated password, which will not be shared with other students. Students can communicate with teachers through Google Classroom. E-mail is not to be used by students on school computers under circumstances other than those described. This includes Google Hangouts and other network/web communication options.

SOCIAL NETWORKING/CHAT ROOMS (including Facebook, Face Time, Twitter, Skype, Hangouts, etc.): Chat rooms and social networking including but not limited to Face Time, Facebook, Skype, Twitter, Hangouts, etc. are not to be used on school computer/devices for reasons other than educational purposes.

FILTERING TECHNOLOGY: TPC has installed and engaged Internet filtering software. This software is employed both in compliance with the *Children's Internet Protection Act* as well as our belief that we must do our best to support our students' learning in a manner that supports TPC's mission and provides for a safe learning environment. Use of filtering software cannot guarantee that all inappropriate sites can never be accessed; however, it drastically reduces that opportunity.

Despite every effort for supervision and filtering, all parents/guardians of TPC students are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every student (to the best of their ability) must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every student (to the best of their ability) must report security or network problems to their teacher and the Integrative Technology Coordinator.

SCHOOL-PROVIDED DEVICES: For the purposes of this Policy, "device" shall include, but not be limited to, portable devices such as computers, laptops, Chromebooks, tablets, cellular telephones, AAC devices, or any other computing or electronic devices TPC provides to students to be used as part of their educational program.

1. Students (to the best of their ability) are expected to report any hardware or software problems in the operation of the device to their classroom teacher or the Integrative Technology Coordinator in a reasonable amount of time.
2. A student shall be subject to consequences in the event the student violates any TPC policy, including the AUP.

PRIVATELY-OWNED TECHNOLOGY: For the purpose of this Policy, "privately-owned" means technology hardware and software that is purchased, owned, and maintained by the student or sending district at no expense to TPC (this may include, but is not limited to, any type of computer, portable devices such as computers, laptops, Chromebooks, tablets, cellular telephones, AAC devices, or any other computing or electronic devices computer device. The use of privately-owned technology by a student in the educational program during the school day must be approved by the student's parent or legal guardian and the school teaching staff member (and/or the Integrative Technology Coordinator) responsible for supervising and/or providing the student's instructional program. A teaching staff member may approve a student's use of privately-owned technology based on the assignment(s) to the student. The teaching staff member may also prohibit the use of privately-owned technology for assignments.

Any use of privately-owned technology by a student shall be in strict accordance with the teaching staff member's specific approval and the Acceptable Use Policy. Any violation will subject the student to appropriate discipline. TPC assumes no responsibility for the security of or damage to any privately-owned technology brought to school by a student.

USER SAFETY: Users are not to post, publish or send personal information about themselves or others, nor are they to engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that student's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

In accordance with the provisions of the Children's Internet Protection Act, the classroom teacher and/or Integrative Technology Coordinator will ensure education is provided to students, as appropriate regarding appropriate online behavior, including interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

ACTIVITIES THAT ARE PERMITTED AND ENCOURAGED:

1. investigation and research in support of school studies
2. investigation and research of opportunities outside of school that are related to community service, employment or college information

ACTIVITIES THAT ARE NOT PERMITTED:

1. searching, viewing, sending or retrieving materials that are not related to schoolwork, community service, employment or college information
2. plagiarism, copying, saving or redistributing copyrighted material. Users should assume that all material is copyrighted unless explicitly noted. Source, author, website source and date

accessed, etc. must be present on any printed copy or inclusion in any paper, on the same basis as using quotes from a textbook or periodical

3. the use of personal devices (e.g. phone, camera, iPad, etc.) to capture still or moving images of students and/or staff
4. any use of TPC computers/devices for financial gain
5. sharing of the users or another's home address, phone number or other personal information
6. unauthorized access, including "hacking," and any activity that violates a school rule or a local, state or federal law
7. searching or viewing sexually explicit, profane, promotion of violence or hate, or illegal materials;
8. forging e-mail messages or using an account owned by others
9. gaining or attempting to gain unauthorized access to the files of others, or vandalizing the data of another user
10. invading the privacy of others
11. posting anonymous messages

Offenses such as threats, theft, and violation of another person's rights will result in prosecution to the full extent of the law.

If anyone has any questions about whether a specific activity is permitted, he or she should ask a teacher or administrator. If you mistakenly access inappropriate information, you should immediately tell the classroom teacher or Integrative Technology Coordinator. This will protect you against a claim of intentional violation of this policy.

TECHNOLOGY RULES OF CONDUCT

HARDWARE, NETWORKS and SERVERS:

1. Never share your password. If a user shares a password with another, that user is as responsible for any ensuing action as the person actually performing the action and will be held accountable.
2. Treat all hardware with respect. Use it in a way that will not cause damage.
3. Do not change settings, configuration, or in any manner make changes to the way a device operates or is viewed.
4. Do not attempt to circumvent any management controls.
5. Unauthorized access including "hacking," and other unlawful activities will be prosecuted.
6. Hubs, routers, servers, or connectors are off-limits to all but IT department staff.
7. Do not adjust, connect, or disconnect components.
8. Do not open school hardware.
9. No food or drink near computer stations or devices.

SOFTWARE/APPS:

1. Always honor copyright laws and licenses.
2. Students are not to install software or mobile/web apps.
3. Staff may install software/apps in cooperation with and consent of the IT department.
4. Do not change, copy, or delete software/apps.
5. Virus protection is provided through the network; however, caution should be used.
6. Do not attempt to circumvent any software controls.

INTELLECTUAL PROPERTY:

You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether you can use a work, you should, direct any questions regarding copyright law to a teacher or the Integrative Technology Coordinator.

RULES FOR COMMUNICATING WITH OTHERS VIA E-MAIL

1. Students may use e-mail only if access is obtained via a GSFE account using Google Classroom.
2. Do not send or display offensive messages or pictures.
3. Do not send e-mail that harasses, insults or attacks others.
4. Do not forge a message or use another's account.
5. Never give out personal information (Name, address, age, etc.) about yourself or others.
6. If you receive inappropriate e-mail, immediately notify teacher or the Integrative Technology Coordinator.

RULES FOR INTERNET USE

1. Sites and materials accessed must be for educational purposes, aligned curriculum studies and support IEP goals.
2. Only files accessed for educational purposes may be downloaded.
3. If you accidentally browse to a web page that is inappropriate:
4. Immediately notify a teacher or the Integrative Technology Coordinator.
5. Do not bookmark or share the addresses of pages that are inappropriate.
6. Never fill out online forms or give personal information about yourself or others.

PENALTIES FOR MISUSE OF TECHNOLOGY

Technology and Internet use is a privilege extended by TPC, and not a right. Breaking any of the rules is therefore a violation of that privilege and will have consequences, which will be enforced by the Principal or designee.

Student disciplinary actions may include, but are not limited to:

1. use of networks/computers only under direct supervision;
2. suspension of network privileges;
3. revocation of network privileges;
4. suspension of computer privileges;
5. revocation of computer privileges;
6. suspension from school;
7. legal action and prosecution by the authorities.

The severity and/or frequency of the offense will determine the consequence ranging from an unspecified length of time to permanent exclusion from technology use.

Questions or concerns please contact:

Katie Passarotti, Principal
The Phoenix Center
16 Monsignor Owens Place
Nutley, NJ 07110
973-542-0743
kpassarotti@thephoenixcenternj.org