

BREAKTHROUGH CHARTER SCHOOL

Children's Internet Protection Act (CIPA) - Compliance Policy

STUDENT COMPUTER ACCESS AND USE

INTERNET SAFETY

In accordance with the *Children's Internet Protection Act (CIPA)*, Breakthrough Charter School shall enforce a policy of Internet safety that incorporates the use of computer-related technology or the use of Internet service provider technology designed to block or filter Internet access to certain visual depictions, including without limitation those that are obscene, child pornography, or otherwise harmful to minors. Sites that are excessively violent, pervasively vulgar, sexually harassing, or that contain information regarding the manufacturing of bombs or other incendiary devices shall also be prohibited. Only authorized persons may disable the blocking or filtering mechanism *for an adult user* in order to enable Internet access for bona fide research or other lawful purposes.

In addition to filtering requirements, it shall be the policy of the School to:

1. Prohibit access by minors to inappropriate matter on the Internet and World Wide Web;
2. Institute measures to ensure the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications, such as "Instant Messaging";
3. Prohibit unauthorized access, including what is now known as hacking, and other unlawful on-line activities by minors online;
4. Prohibit unauthorized disclosure, use, and dissemination of personal information regarding minors; and
5. Institute measures designed to restrict minors' access to materials harmful to minors.

PERMISSIONS

1. The Student Technology Usage Agreement shall be distributed to the student and parent/guardian and will be posted on the School web site.
2. Students and Parent/guardians are required to sign the Student Technology Usage Agreement. The student and parent/guardians signatures shall be **legally binding** on all

parties and shall indicate they have read the terms and conditions carefully and understand their significance.

3. Parental/guardian permissions that are assumed include:

- Access to the Internet
- Permission to publish students' work to classroom web sites
- Permission to have unidentified photos of students published to classroom web sites

COMPUTER AND INTERNET USE TERMS AND CONDITIONS

1) *Acceptable Use* - The purpose of the Internet is to support research and education in and among academic institutions in the United States by providing access to unique resources and opportunities for collaborative work. Transmission of any material in violation of any U.S., state, local, or School regulations shall be prohibited.

2) *Netiquette* - Users shall be expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Be polite. Do not send abusive messages to others. Use appropriate language.
- Do not reveal personal addresses or phone numbers of students or colleagues.
- Note that Electronic Mail (EMail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities must be reported to the authorities. All users should be aware that routine monitoring of the system may lead to the discovery that the user has or is violating the Acceptable Use Agreement, the Student Handbook, and/or the law. Routine maintenance of the system may also purge files from individual accounts.
- Do not use the network in a way that would disrupt the use of the network by other users (e.g. downloading huge files during prime time, sending mass email messages, or annoying other users using the talk or write functions). Hardware or software shall not be destroyed, modified, or abused in any way.
- Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system shall be prohibited.
- Hate mail, harassment, discriminatory remarks, and other antisocial behaviors shall be prohibited on the network.
- The illegal installation of copyrighted software for use on School computers shall be prohibited.
- The use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network (LAN) shall be prohibited.

3) *Privileges* - The use of the Internet is a privilege, not a right, and inappropriate use shall

result in a cancellation of those privileges and may result in disciplinary or legal action by the administration, faculty, or staff.

- 4) *Security* - Security on any computer system is a high priority, especially when the system involves many users. Any suspected security problem on the Internet shall be reported to the Head of School, who shall immediately contact the Director of Technology or designee. Any user identified as a security risk or having a history of problems with other computer systems shall be denied access to the Internet.
- 5) *Vandalism* - Vandalism shall result in cancellation of privileges and or other disciplinary actions up to and including expulsion. *Vandalism* is defined as any malicious attempt to harm or destroy hardware or software data of the school system, another user, the Internet Service Provider, or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses, "Digital Graffiti", defacing Websites, unauthorized changes to websites, programs, applications, databases, etc. No software, programs, or files may be installed or downloaded by any user without the prior permission of the building technology coordinator, who must scan for appropriateness and viruses.
- 6) *Consequences of Misuse* - The Head of School and/or School Administrators may discipline (up to and including expulsion) any student who accesses, sends, receives, or configures electronically any profane language or pictures or violates any School policy.

RESPONSIBLE USE / CODE OF CONDUCT

Students at Breakthrough Charter School may not use the network or any school's computer facilities for hate mail, defamatory statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Honesty, integrity, and respect for the rights of others should be evident at all times. E-mail shall be limited to teachers and whole classes. Individuals shall not have accounts unless specifically authorized by the parent. Students shall only be identified by first names.

The use of the Internet, including the World Wide Web, must be in support of education and academic research and consistent with the educational objectives of Breakthrough Charter School. The School shall not be responsible for any financial obligations incurred by users of the Internet.

Cyberbullying shall result in cancellation of privileges and or other disciplinary actions up to and including expulsion. Any validated reports of cyberbullying which contain true threats of intent

to harm a person will be reported to law enforcement. The test of “intent to harm” is whether a reasonable person sending a communication would foresee that the listener would interpret the statement as a serious expression of intent to harm.

The computer user shall be held responsible for his/her actions and activities. Unacceptable uses of the computers and/or the Internet shall result in appropriate disciplinary action, including suspension, expulsion, or revoking of these privileges. If a student has questions about whether a specific activity is permitted, he or she should ask a teacher or administrator.

If a student accidentally accesses inappropriate material, he or she should back out of that information at once. Students who may inadvertently access a site that is pornographic, obscene, or harmful to minors shall immediately disconnect from the site and inform the teacher.

Students shall use the Internet search engines and/or other Internet tools only under the direction and supervision of teachers.

Regulations for the use of computers and the participation by anyone on the Internet include but are not limited to, the following:

1. Student use of e-mail and other forms for direct electronic communication including instant messaging systems is prohibited unless authorized and directly supervised by a teacher.
2. School system rules prohibiting cyberbullying indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing language applies to all forms of electronic communications.
3. Students shall not post any e-mail or other messages or materials on school or School networks or the Internet that are indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing.
4. Students shall not post personal information about themselves, (last name, addresses, or telephone numbers) or any other person.
5. Students shall not abuse or waste network resources through frivolous and non-educational use or send chain letters or annoying or unnecessary letters to large numbers of people.
6. Students shall not access over the Internet visual depictions that are obscene, pornographic, or harmful to minors.
7. Students shall not attempt to gain unauthorized access, including so-called "hacking" or otherwise compromise any computer or network security or engage in any illegal activities on the Internet, including willfully introducing a computer virus, worm, or other

harmful programs to the network.

8. Students shall observe copyright law and fair use guidelines. Students shall not plagiarize or otherwise use copyrighted material without permission. Students shall properly cite the source of information accessed over the Internet.
9. Students shall not make any purchase on the Internet while using school equipment or Internet service.
10. Degrading or disrupting equipment or system performance shall not be permitted.
11. Invading the privacy of individuals, sending of hate mail, harassing, or making discriminatory remarks or other antisocial behavior shall be prohibited.
12. Using an account owned by another user shall be prohibited.
13. Posting anonymous messages shall not be permitted.
14. Perusing or otherwise accessing information on manufacturing bombs or other incendiary devices shall be forbidden.
15. Downloading information without the permission of the Head of School or designee shall be prohibited.
16. Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that taken as a whole and with respect to minors, appeals to the prurient interest in nudity, sex, or excretion shall be prohibited.
17. Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that describe or represent in an offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals shall be prohibited.
18. Accessing or creating exposure in any way to pictures, graphics, or other visual depictions that taken as a whole lack serious literary, artistic, political, or scientific value as to minors shall be prohibited.
19. Use for product advertisement, political lobbying, or illegal activities shall be strictly prohibited.
20. Social Media websites will be restricted.
21. Subscriptions to list servers, bulletin boards, and online services must be pre-approved by the Superintendent or his/her designee.

CIPA MONITORING AND TRAINING

In addition to the use of technology protection measures, the monitoring of student's online activities and access to the Internet and World Wide Web may include, but shall not be limited to, the following:

1. Ensuring the presence of a teacher and/or other appropriate School personnel when students are accessing the Internet including, but not limited to, the supervision of students when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail and chat rooms, instant messaging and other forms of direct electronic communications may be blocked as deemed necessary to ensure the safety of such students.
2. Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors.
3. Provide annual training regarding CIPA policy to all students and faculty. Training for students and faculty will address key issues such as cyberbullying, social networking dangers, and emerging technologies that may endanger children while using the Internet. Teachers will train students by incorporating within their lesson plans age-appropriate Internet Safety training for students. The Head of School or the designated representative will periodically review lesson plans to ensure all students are trained.