

STUDENT COMPUTER ACCESS AND USE

Children's Internet Protection Act Compliance Policy

Virgil Browne Glencoe Charter School

INTERNET SAFETY

The Internet is a vast, global computer network that provides access to major universities, governmental agencies, other school systems, and commercial providers of data banks. Virgil Browne Glencoe Charter School School Board shall establish appropriate guidelines for exploring and using Internet resources within the school district to enhance learning and teaching activities. Acceptable use of these resources shall be consistent with the philosophy, goals and objectives of the Virgil Browne Glencoe Charter School School Board. All elementary schools beginning with the third grade and all secondary schools shall provide instruction for educating children regarding Internet safety.

In its continued efforts to comply with the *Children's Internet Protection Act*, the School Board shall adopt and 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 for minors and adults to certain visual depictions, including without limitation those that are obscene, child pornographic, or harmful to minors, including without limitation sites that are excessively, violent, pervasively vulgar, or sexually harassing. Sites which contain information on the manufacturing of bombs or other incendiary devices shall also be prohibited. Only authorized persons may disable for an adult user the blocking or filtering mechanism in order to enable Internet access for bona fide research or other lawful purposes, which shall include online services for legitimate scientific or educational purposes approved by the Board, or access to online services of a newspaper with a daily circulation of at least 1,000.

In addition to filtering requirements, the Board shall maintain regulations which:

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

PERMISSIONS

- 1) The *Student Computer Access and Use* policy shall be distributed to the student and parent/guardian through the school handbook and shall be posted on the School Board web site.
- 2) Parental permission shall be assumed unless specifically denied. *Denial of Permission Forms* are available at all schools.
- 3) Parental/guardian permissions that are assumed include:
 - Access to the internet and email system
 - 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 District regulations shall be prohibited.
- 2) *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.
- 3) *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 building technology coordinator or the principal, 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.
- 4) *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 Internet. This includes, but is not limited to, the uploading or creation of computer viruses. 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.
- 5) *Consequences of Misuse* - School principals may discipline (up to and including expulsion) any student who accesses, sends, receives, or configures electronically any profane language or pictures or violates the *Code of Conduct* for computer use, or any rules contained in the *Acceptable Use Agreement*.
- 6) *Cyberbullying*: Cyberbullying shall result in cancellation of privileges and or other disciplinary actions up to and including expulsion. Cyberbullying is defined as the use of

the Internet to harass or bully others. Virgil Browne Glencoe Charter School is a place of tolerance and good manners. Students 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.

RESPONSIBLE USE

Virgil Browne Glencoe Charter School School Board *Student Code of Conduct* applies to all persons who use any School Board computer. Honesty, integrity, and respect for the rights of others should be evident at all times.

The use of the Internet, including the World Wide Web, in Virgil Browne Glencoe Charter School school must be in support of education and academic research and consistent with the educational objectives of the Virgil Browne Glencoe Charter School School Board. Neither Virgil Browne Glencoe Charter School School Board nor the school shall be responsible for any financial obligations incurred by users of the Internet.

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 school 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.

In general, any student use of networks and telecommunications resources must be for educational purposes and conform to school system rules of behavior. *Regulations for the use of computers and the participation by anyone on the Internet shall include but not be not be 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 indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing language apply to all forms of electronic communications.
3. Students shall not post any e-mail or other messages or materials on school or district 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 program 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 permission of the Director of Technology 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. Subscriptions to list servers, bulletin boards, and on-line services must be pre-approved by the Superintendent or his/her designee.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Technology or designated representatives.

Ref: 47 USC '254(h), *Children's Internet Protection Act* (CIPA); La. Rev. Stat. Ann. ' '17:81, 17:100.7, 17:280.