CTA Internet Safety and Acceptable Use Policy

This document defines for students the acceptable use of the CTA network system (i.e. WAN, LAN, Internet, email, computer, and other technological resources). Following this policy allows students to use the Internet in a safe and responsible manner.

1. PURPOSE

(a) The school's network system has been established for educational and administrative purposes. The term "educational purposes" includes classroom activities, continuing education, professional or career development, and high quality, educational-enriching personal research.

(b) The school's network system has not been established as a public access service of a public forum. The school has the right to place restrictions on the material which students access or post, though students are also expected to follow the rules set forth in this policy, the student disciplinary code, and the law in their use of the School's network system. Staff members are obligated to hold students accountable, and disciplinary procedures may be taken for those who breech the rules established.

(c) Students may not use the school's network for commercial purposes. This means students may not offer, provide, or purchase products or services through the school's network system unless it is directly related to a business project with adult permission and oversight.

(d) Cross Trainers Academy staff have a responsibility and obligation to take all reasonable measures to protect children and provide a safe online environment. Internet safety training will be provided to our students, including lessons that address appropriate online behavior, cyberbullying awareness and response, social networking sites and chat rooms. It shall be the responsibility of Cross Trainers Academy staff to supervise usage by minors of the online computer network and access to the internet in accordance with this policy and the Children's Internet Protection Act.

2. ACCESS TO ONLINE MATERIALS

(a) The material which students access through the school's network system should be for class assignments or for personal research on subjects similar to those that a student might study in a class or in the school library. Use for entertainment purposes is not allowed.

(b) Students shall not use the school's network system to access the following:

1. Material that is obscene;
2. Pornography, including child pornography;
3. Material that depicts, or describes in an offensive way violence, nudity, sex, traumatic death or bodily functions.
4. Material that has been designated as for adults only;
5. Material that promotes or advocates illegal activities;
6. Material that promotes the use of alcohol or tobacco or school cheating or material that advocates participation in potentially dangerous groups.

7. Material that is deemed harmful to minors.

(c) If a student mistakenly accesses inappropriate information, he/she should immediately report this access in the manner specified by his/her school. This will protect the claim that he/she has intentionally violated this policy.

(d) The school has installed technology protection measures to block access to inappropriate material and to visual depictions deemed obscene, child pornography, or harmful to minors.

Students or staff members should not seek to bypass the filtering software by using a proxy site or some other technology.

(e) New technologies are being invented constantly, and it is impossible to predict what systems or applications will be available for use in the future. This policy applies to all technologies currently in use on the school network, as well as those technologies that may be used on the school's network in the future.

3. SYSTEM SECURITY AND RESOURCE LIMITS

(a) You are responsible for your individual account and should take all reasonable precautions to prevent others from being able to use your account. You should change your password regularly. Under no conditions should you provide your password to another person. You should always log off the computer when you are finished.

(b) You will immediately notify the principal or administrator if you or another person has identified a possible security problem. However, do not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

(c) You will avoid the inadvertent spread of computer viruses by following the district virus protection procedures.

(d) You will request permission to download applications. Cautiously approach downloads and do not use suspicious or unprotected sites.

4. COMMUNICATION SAFETY

The school will not guarantee that the functions or services provided through the network system will be without error. The school will not be responsible for any damage you may suffer, including but not limited to loss of data, interruptions of service, or exposure to inappropriate material or people. The school will not be responsible for the accuracy or quality of the information obtained through the network system. The school will not be responsible for financial obligations arising through the unauthorized use of the system.

5. UNLAWFUL, UNAUTHORIZED AND INAPPROPRIATE USES

(a) You will not attempt to gain unauthorized access to the school's network system or go beyond your authorized access. This includes attempting to log in through another person's account or to access another person's files.

(b) You will not make deliberate attempts to disrupt the school's system or destroy data by spreading computer viruses or by any other means.

(c) You will not use the school's system to engage in any other unlawful act, including but not limited to; arranging for a drug sale or the purchase of alcohol or weapons, engaging in criminal gang activity, or threatening the safety of any person.

6. INAPPROPRIATE LANGUAGE

(a) Restrictions against inappropriate language apply to all speech communicated through the school's network system, including public messages, private messages, and material posted on Web pages, wikis, and blogs or any other social networking sites.

(b) You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

(c) You will not engage in slander, bullying, or other harassing, or derogatory email messages, instant messages, text messages, digital pictures, use of crude or vulgar language including profanity, or derogatory images or website posting.

(d) You will not post information that could cause damage or a danger of disruption to your school or the people in the school. This includes knowingly posting false or offensive information about a person or organization.

(e) You will not engage in copyright infringement or plagiarism.

7. PRIVACY

(a) There is no expectation of privacy in files kept on the school's network system, school-owned technology and records of your online activity when using school-owned technology or the school's network system.

(b) The school will cooperate fully with local, state, and federal officials in any investigation related to any unlawful activities conducted through the school's network system.

(c) CTA may monitor student online activity when using school technology or the school's network system.

8. MONITORING STUDENTS

(a) Students should not be left unsupervised at any time where internet access is available. Teachers are the primary supervisors, but other staff member and volunteers are also accountable to maintain alertness and vigilance while monitoring students so that they are not purposefully or inadvertently subjected to offensive materials.

(b) All accidental and intentional misuse of technology should be reported to the principal or administrator immediately.

(c) At all times it is expected that Biblical principles override all aspects of both adult and student use of technology and communication.

9. DAMAGED TECHNOLOGY

(a) All equipment must be correctly closed, opened, charged, and locked. Adults are expected to check in their equipment in good condition and return in the same condition. Damage and viruses must be reported immediately.

(b) Damage that occurs for recklessness, carelessness, or clumsiness will be the responsibility of the user to repay in full.

Consequences for Violation of the Acceptable Use Policy:

Consequences for violating the Acceptable Use Policy for school technology and technology resources (hardware, software, and online internet) will be determined on a case-by-case basis. Consequences could include, but are not limited to:

- Warning
- Detention
- Parent meeting
- In-school suspension (Resilience Room)
- Out-of-school suspension
- Short-term removal of technology use privileges
- Permanent removal of technology use privileges
- Fees assessed to the family of the student for damage to school technology/equipment
- Work detail (e.g. cleaning cafeteria, cleaning garbage from campus).
- Expulsion

Consequences will depend on the nature of and/or severity of the infraction.

I have read and agree to the ACCEPTABLE USE POLICY for ALL TECHNOLOGY at Cross Trainers Academy. I acknowledge that breaking the rules found in this policy is grounds for termination of my position at Cross Trainers Academy if I am a staff member and grounds for expulsion if I am a student.

Student name (print first and last name): ______________________________________

Student signature: ____

Today's Date: ______________________

Parent/Guardian Signature: ____

Today's Date: ______________________

Please sign, date and return this form as part of your CTA enrollment/ registration packet. You will receive a full copy of this school technology policy inside the CTA Student/Parent Handbook that is issued to every family each school year. This policy is also posted on the Milwaukee Rescue Mission/CTA public website @ www.milmission.org