MONTACHUSETT REGIONAL VOCATIONAL TECHNICAL SCHOOL

INTERNET SAFETY

Monty Tech is committed to insuring the highest standards of online safety for all of our students. The staff and administration at Monty Tech take very seriously our obligation to insure that our students are protected from websites and computer resources that are not appropriate.

This document explains what Monty Tech does to protect our students and areas where we think parents and guardians should be concerned regarding the safety of our students when they are using the Internet.

Content Filtering

The Children's Internet Protection Act (CIPA) and other federal regulations require that websites containing inappropriate content be blocked. Monty Tech complies with these regulations by using a content filtering system that stops websites with obscene, sexually explicit, or other educationally inappropriate material that may be deemed harmful to minors before they enter our network. This type of filtering is done automatically. However, we feel we also have an obligation to insure our students are protected from "social networking" and other situations that might jeopardize a student's safety. The district will monitor the online activities of minors.

Websites that do not fall under the guidelines above but are nevertheless inappropriate in an educational environment are blocked. Monty Tech blocks social networking websites such as facebook.com and twitter.com, as well as chat room and instant messaging type websites. Although these websites may not be illegal, these types of websites have often been associated with stalking, harassment, and bullying and, therefore, are blocked. Monty Tech also restricts electronic email to Monty Tech provided email accounts. All messages are archived.

Acceptable Use Policy

Monty Tech has an Acceptable Use Policy (AUP) that outlines guidelines for acceptable use of our computer network and resources. A summary of the AUP can be found in the Student Handbook, and the full AUP can be found on Monty Tech's website: www.montytech.net. Disciplinary action will be taken for unauthorized access, including "hacking", and other unlawful activities by minors online as well as unauthorized disclosure, use, and dissemination of personal information regarding minors.

Guidelines

The best protection against unauthorized use of an email account or social network website account is to not share the username or password with friends or acquaintances. It is recommended that the password be a combination of letters, numbers, and/or symbols so that the password is not easy to guess. It is also important to log out of the account and close the Internet browser when using someone else's computer, including computers in a public place like a library. Never save your password on a public computer.

Social network websites, such as facebook.com, allow individuals to create profiles, post pictures and talk to friends online. Problems ensue when teens post too much information about themselves and others, including phone numbers, addresses, where they are going, and even information that may be incriminating. If privacy settings are not set correctly anyone, not just friends, can see the information, including the pictures.

Teens are often drawn into chat rooms by people who misrepresent themselves, with the intent of luring the teen into a harmful situation.

Cyberbullying also occurs on social network websites. The bullying can include physical threats, but more typically involves spreading malicious lies and rumors. Again, anyone may be able to read posts and further spread falsehoods.

Please note that many employers and universities now check social network websites to see what an applicant says about himself/herself. A picture taken at a wild party may not be the impression you want to give.

Guidelines for teens:

1. Never provide the following information about yourself online without first checking with your parent/guardian: home address, telephone number, birthday, school, passwords, or photographs. Limit the information on your profile, and do not post pictures of yourself or friends at school events.
2. Never go alone to meet someone you know only from the Internet. Tell a trusted adult if someone asks you to meet them, even if it is in a public place.
3. Never tell someone you are alone at home.
4. Do not tell anyone anything online that you would not want others to know.
5. If you are made uncomfortable in a chat room, leave it. Do not put up with rudeness, bullying, or provocative chat.
6. Report threatening, harassing, or abusive messages or pictures to your parent/guardian or the police. If there is a reference to Monty Tech, give a copy to the Dean of Students.
7. Do not answer threatening or obscene email or chat room messages.
8. Do not download anything unless it is from a trusted source. Do not click on links in an email or open an email attachment unless the message is from someone you know. The link or attachment may contain a virus or program that will search your computer for user names and passwords.
9. It is illegal to threaten, harass or bully someone over the Internet or phone.
10. It is illegal to send graphic photos to someone under the age of 18.
11. It is illegal to use someone else's identity without permission, including logging on to someone else's account.

Guidelines for parents:

1. Supervise the use of the Internet. Place the computer in a common area of the house where adults are able to monitor its use.
2. Set reasonable expectations for online behavior.
3. Become familiar with the privacy settings on social network websites, and work with your teen to restrict information.
4. Talk to your teen about online interests and friends, and ask to see the websites he/she visits.
5. Tell your teen to report messages that contain obscene material or threatening messages to your Internet service provider and the police.
6. Consider installing filtering software to block unwanted messages and access to objectionable websites.