Overview of Computer Use

All students assume the following responsibilities concerning the use of Mt. Vernon Township High School technology:

1. It is the student’s responsibility to treat all equipment with care and to report instances of abuse or misuse as soon as the student becomes aware of them to a teacher or staff member. Each student is expected to report any malfunction or problem, immediately upon discovery, to a teacher, Technology Services Department staff member or School Administrator.

2. In the event that a student vandalizes or otherwise intentionally damages any District computer hardware or software, he/she (or legal parent/guardian if the student is a minor) will be responsible to pay all repair and/or replacement costs. Vandalism is defined as any malicious attempt to harm or destroy data of another student, school software, the Internet, the Network, computer hardware, computer wiring, and computer configuration. This includes, but is not limited to, the uploading or creation and distribution of computer viruses. By signing the Computer and Internet Acceptable Use Policy Acknowledgement form at the end of this document, the parent/guardian expressly agrees to be responsible for payment of costs incurred. The student will be referred to the building principal or district administration for appropriate discipline, including but not limited to, suspension from or denial of access to all District computers.

3. Any student who damages, destroys, or copies another person’s data will be referred to the principal for appropriate discipline and may be suspended from or denied access to all computers. Incidents in which a student copies another student’s data will be treated as cheating, and will be handled per student handbook.

4. Any student who tampers with or attempts to gain access to computer data to which he/she has no specific security authorization is in violation of district policy. It will be considered equivalent to tampering with a teacher’s written records or attempting to gain access to confidential student information.

5. A student will not load or copy unauthorized software, to include music, video and games, onto District computers. All software used on District computers and networks is to be properly licensed and registered and installed by Technology Services Department personnel. If found student subject to discipline as to handbook.

6. Network security and student safety are high priorities. If a student can identify a security problem on the district network and/or Internet, he/she must notify the Technology Coordinator or principal. The student should not demonstrate the problem to other students. The student should keep all account and password information confidential. The student should not use another student’s account. Each student is responsible for any network activity conducted under their account. All network users have no expectation of privacy in any material that is stored, transmitted, or received via the District’s electronic network or District computers. Attempts to connect to the district network, building network or the Internet as a system administrator will result in cancellation of student privileges and appropriate disciplinary and/or legal action. Any student identified as a security risk may be denied access to the network.

7. Teachers and staff are instructed to monitor and supervise all students, in the classroom or in a lab setting. When students are participating in an online activity they are not to be engaged in inappropriate activities such as; attempts to bypass district content filtering (proxy sites), conduct of unlawful activities, hacking attempts upon onsite or offsite data servers or network equipment, or attempts to alter their own, or other student’s information or data. Teachers and staff will also limit student usage of personal e-mails to classroom and school related activities. Participation in online chat rooms or other social networking sites is prohibited.
Internet Safety And Use

Each District computer shall access the Internet through a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) considered harmful or inappropriate for students, as defined by the Children’s Internet Protection Act and as determined by the Superintendent or Superintendent’s designee. The Superintendent or said designee shall enforce the use of such filtering devices. An authorized Technology Services Department administrator may disable the filtering device for instances of bona fide research or other lawful purpose, provided permission is granted by the Superintendent or network administrator. The Superintendent or designee shall include measures in this policy’s implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized and inappropriate access, including “hacking” and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Students who have parental consent may access the Internet. While no filtering software provides 100% security from inappropriate sites, it is the district’s policy that students using the Internet will be monitored by district staff at all times.

Authorization For Electronic Network Access

Each student and his or her parent(s)/guardian(s) must sign the Computer and Internet Acceptable Use Policy Student and Parent Acknowledgement form before being granted access to the District’s Electronic Network. This form will only have to be filed out once while the student is enrolled.

All use of the District’s Electronic Network shall be consistent with the District’s goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This policy does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided.

The failure of any user to follow the terms of the Computer and Internet Acceptable Use Policy may result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Employees have no expectation of privacy in their use of the District Electronic Network. The District has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the District’s electronic mail system. The District has the right to and does monitor use of the District Electronic Network by students, including students’ access of the Internet, as part of maintenance and to determine whether the use is consistent with federal and state laws and District policies and guidelines.

Employees should be aware that their personal computer files or System use may be subject to public disclosure under the Illinois Freedom of Information Act.

Inappropriate Internet Use

The following list includes examples of inappropriate Internet use, but is not limited to.

1. Intentionally accessing content that is inappropriate in a school environment, or submitting, posting, publishing or displaying any defamatory, abusive, obscene, profane, pornographic, threatening, racially offensive, harassing, religious or illegal materials, or material of a sexual nature, that is inappropriate in a school environment (unless the topic is a research assignment specifically authorized by a teacher):

   Alcohol | Libelous or Slanderous Material
   Bomb Making | Militants and/or Extremist Students or Groups
   Deviant Social Behavior | Pornography and/or Sexually Oriented Material
   Gambling | Profanity
   Gangs | Racism
   Human or Animal Mutilation | Satanic Themes and/or Religious Cults
   Illegal Activity | Tobacco
   Illegal Drugs | Violence or Weapons

2. Downloading information and/or software to a school server drive or a computer's hard drive (unless specifically authorized to do so by a teacher or other school personnel).

3. Downloading and/or installing “hacker” programs—programs that are designed to “sniff” or break network or computer station security.

4. Sending or forwarding Email that contains profanity, threats or other inappropriate content.

5. Failing to exit the Internet, shut down, or log off a computer after being instructed to do so by school personnel.

6. Receiving or sending information in violation of U.S. copyright or other state and federal regulations.
7. Electronically harassing or stalking another person by means of the Internet and/or Email.

8. Possessing and/or electronically transmitting another person’s district account or password information.

9. Gaining access to the district network under a staff member's or network administrator's account.

10. The loaning or sharing of login names and passwords to any individual.

11. Gaining access to the district network under another student’s account with or without the other student’s consent.

12. Using school computers and/or the Internet after having access removed by school personnel.

13. Accessing and/or transmitting messages via an electronic "chat room" (unless under direct teacher supervision when the chat room is used for educational purposes consistent with district objectives).

14. Forging official school documents, forms and/or identification cards.

15. Authoring and/or editing, FROM SCHOOL DISTRICT EQUIPMENT, district or personal web pages that contain any nudity or pornography; copyright infringement; material that is threatening, abusive, harassing, defamatory, invasive of privacy or publicity rights, vulgar, obscene, profane, indecent, or otherwise objectionable; content that promotes, encourages, or provides instructional information about illegal activities—specifically hacking, cracking, or phreaking, including posting other peoples’ or district private information; and any software, information, or other material that contains a virus, "Trojan Horse", "worm" corrupted data, or any other malware or harmful or damaging component; hate propaganda or hate mongering, swearing, or fraudulent material or activity.

16. Authoring, editing and/or transmitting computer viruses to/from/via school district equipment.

17. Transmitting personal information to an Internet “stranger” or unreliable/unknown organization, group, etc.

18. Posting or transmitting material created by another person without his/her consent.

19. Posting or transmitting anonymous messages.

20. Modifying or attempting to modify Web sites without authorization.

21. Accessing or attempting to gain access to restricted sites without authorization.

22. Ordering goods or services by means of the Internet and/or Email with a credit card or other methods of payment.

23. Soliciting and/or conducting business by means of the Internet and/or Email for personal financial or commercial gain.

This list is not all-inclusive. Any other misuse of the Internet or the district’s electronic network system, deemed inappropriate by school personnel, may result in disciplinary action and/or appropriate legal action.

Violations of Computer and/or Internet Use

The failure of any student to follow the terms of the Mt. Vernon Township High School’s Computer and Internet Acceptable Use Policy will result in lost or restricted computer use (including Internet access), disciplinary action and/or appropriate legal action. The Superintendent or designee and/or the Principal will make all decisions regarding whether or not a user has violated the Computer and Internet Acceptable Use Policy and may deny, revoke or suspend access at any time.

Any student who loses his/her computer use privileges due to a violation of the Mt. Vernon Township High School, District 201’s Computer and Internet Acceptable Use Policy may be removed from courses that require extensive use of computers and may be subject to disciplinary action, in accordance with board policy.

References

Children’s Internet Protection Act, P.L. 106-554., 20 U.S.C § 6801 et seq., 47 U.S.C. § 254(h) and (l), 720 ILCS 135/0.01.


105 ILCS 5/10-20.14 Student Discipline Policies; Parent-Teacher Advisory Committee

Public Input

MVTHS will provide public notice for, and hold at least one public meeting, in order to address any proposed modification of the district’s Electronic Network and Internet Safety Policy. This meeting may be held in conjunction with other school business. This meeting will observe the Illinois Open Meetings Act.
MT. VERNON TOWNSHIP HIGH SCHOOL
Technology Services Department

Computer and Internet Acceptable Use Policy
Student/Parent Acknowledgement Form

Student Acknowledgement

I understand and will abide by the preceding Computer and Internet Acceptable Use Policy. I further understand that should I commit any violation, my access privileges may be revoked, and disciplinary action and/or appropriate legal action may be taken.

→ __________________________
Student’s Name (please print)

→ __________________________
Student’s Signature
Date

Parent/Guardian Acknowledgement

Parental Permission for Computer Use: I have read the above Computer and Internet Use Acceptable Use Policy. I have discussed the terms of the Rules and Regulations with my son/daughter. I hereby request that my son/daughter be allowed access to the district’s computers.

→ __________________________
Parent/Guardian Name (please print)

→ __________________________
Parent/Guardian’s Signature
Date

Parental Permission for Internet Use: I understand that the District’s computer access to the Internet is designed for educational purposes and that the District has taken precautions to protect students from inappropriate Internet sites, including the use of filtering/blocking software and staff monitoring. However, I also recognize that filtering software cannot block every controversial and inappropriate Internet site. In the unlikely event that a student accesses, either intentionally or unintentionally, inappropriate Internet material, I will hold harmless the District, its employees, agents and Board members for any harm caused by this material. I hereby request that my child be allowed access to the Internet through the District’s connection.

→ __________________________
Parent/Guardian Name (please print)

→ __________________________
Parent/Guardian(s) Signature
Date