COMPUTER NETWORK ACCEPTABLE USE AND INTERNET REGULATIONS

The Merton Community School District recognizes the importance of computer technology as an integral part of the teaching/learning process. The purpose of this document is to provide guidelines for acceptable and appropriate use of the computer system. The computer system will include access to a menu of appropriate software related to specific subjects in the school curricular, word/data processing, research tools, voice mail, problem solving, etc. The system will also allow access to the vast resources available on the Internet World Wide Web. Electronic mail (e-mail) is also an integral part of the schools' computer network.

Students are responsible for good behavior on school computer networks just as they are in the classroom or the school hallway. Communications on the computer network are often public in nature. As a result, the general school rules for behavior and communications apply.

The network that is provided by the Merton Community School District is intended for research, to create documents, and enable communication. Independent access to the network is provided to those students that agree to act in a considerate and responsible manner. Parents may deny access to minors by contacting the Technology Department in writing as to their wishes.

The Merton Community School District makes no warranties of any kind that the function or services provided through the district's computer system will be error free or without defect. The district and its employees will not be held responsible for loss of data or disruption of service. The district will not be responsible for financial obligations arising through the unauthorized use of the district's system.

Access is a privilege, not a right. **Access entails responsibility.**

Users of the Merton Community School District computer network have a limited privacy expectation n the contents of their personal files. The district may conduct a search of an individual's files if there is reason to believe that the user may have violated the law or the district's user guidelines. Parents will also have the right to investigate contents of their child's personal files. Should occasion require, the district will fully cooperate with local, state, or federal officials in any investigation related to any illegal activities conducted through the district's system.

Use of the district's computer network system is considered a privilege and not a right. All users of the system are expected to abide by guidelines to help insure that the system is not used for illegal, illicit, immoral or other inappropriate uses. Unacceptable uses of the network will result in revocation of privileges, suspension, or other disciplinary actions depending on the severity of the violation.
Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.

Computer Network:

1. Use of the Merton Community School District's Computer Network must be in support of the educational development and instruction of the students.
2. Students MUST receive permission to use the computers from the staff member responsible for supervising a room containing computers. In addition, computer use is to stop IMMEDIATELY if the staff member in the room can no longer supervise the use of those computers.
3. ANY use of the computers for illegal activity is strictly prohibited.
4. The illegal installation of software for use on district computers is strictly prohibited.
5. Use of another student's user login name and password is strictly prohibited.
6. Users will not attempt to gain unauthorized access to the district's system or to any other computer system through the district's system. Network accounts, user names, and passwords are to be used only by the authorized person for authorized purposes.
7. Purposely attempting to disrupt the use of the network/computers or attempting to modify, damage, or destroy hardware or software is prohibited.
8. Downloading or adding executable programs is prohibited.
9. Intentionally wasting limited resources is prohibited.
10. Unauthorized use of an outside e-mail account is prohibited.
11. Using or accessing programs that are not licensed by Merton Community School District is prohibited.
12. Changing wallpaper, screen savers or other functions of the pre set computer settings are prohibited.

Internet Access:

During school, teachers of younger students will guide them toward appropriate materials.

1. No electronic mail messages may be sent out of the district network without the permission of the supervising staff member.
2. Use of the Network to engage in illegal activities is prohibited.
3. Use of the Network to access chatrooms, BBS systems, and other networks without the direct supervision of a staff member is prohibited.
4. Use of the Merton Network to access obscene material is prohibited.
5. No Merton Network user may subscribe to receive automated email updates from any website, email list, or listserve.
6. Use of the Internet to obtain information intended for malicious activity is prohibited.
7. Use of the Internet for activities that go outside of the direct guidance of the classroom teacher must be pre-approved by the supervising staff member.

Filtering Policy/Protocol

1. Inappropriate material

a. The District has identified the following types of material as Prohibited, Restricted, and Limited Access Material.

i. Prohibited Material. Prohibited Material may not be accessed by the students or staff at any time, for any purpose. According to the Children's Internet Protection Act the district designated the following types of materials as Prohibited: Obscene materials, child pornography, material that appeals to an inordinate, offensive, or unhealthy interest in violence, nudity, sex, death, or bodily functions, material that has been designated as for "adults" only, and material that promotes or advocated illegal activities.

ii. Restricted Material: Restricted material may only be accessed by students in the context of specific learning activities that have been approved by a teacher or staff member for legitimate research or professional development purposes. Materials that may arguable fall within the description provided for Prohibited Material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be Restricted. In addition, Restricted Material includes materials that advocate the use of alcohol, tobacco, hate, discriminations, school cheating, and weapons.

iii. Limited Access Material. Limited Access Material is material that is generally considered to be non-educational or entertainment. Limited Access Material may be accessed in the context of specific learning activities that are directed by a teacher or during periods of time that a school may designate as "open access" time. Limited Access Material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investments.

b. It is to be understood that the filter is not a foolproof tool in screening out unwanted information. The plain facts are that no approach will ever be successful in totally preventing children using the Internet from accidentally or intentionally accessing inappropriate material or coming into contact with a dangerous individual. Such risks are inherent with the use of the technology. If a user inadvertently accesses material that is considered Prohibited or Restricted, he/she should immediately disclose the inadvertent access in a manner specified by the District.

c. The determination of whether material is Prohibited, Restricted, or Non-educational shall be based on the content of the material and the intended use of the material.

d. Users have limited privacy expectations in the contents of their personal files and records of their online activity while on the district system. Users will be fully informed about the district's supervision and monitoring and the limitations on their privacy that are a result of such supervision and monitoring.

e. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating district policy, regulations, or the law. An individual search will be conducted if there is a reasonable suspicion that a user has violated district policy, regulations, or the law. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

The following behaviors are examples not permitted on the district network:

1. Intentionally wasting limited resources such as online games that are not educational in nature.
2. Email sent to others that has no apparent value.
3. Sending or displaying offensive messages or pictures.
4. Assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition.
5. Using obscene language.
6. Harassing, insulting, or attacking others.
7. Engaging in practices that threaten the integrity of the network. (e.g. loading files that may introduce a virus).
8. Violating copyright laws or plagiarism laws.
9. Trespassing in others' folders, documents, or files.
10. Employing the network for commercial purposes.
11. Violating regulations prescribed by the network provider.
12. Other behaviors in violation of district policy or regulations.

This is by no means a complete list of the activities that may fall in the category of inappropriate use.

Violations will result in disciplinary actions and the proper authorities will be contacted, whenever appropriate.

Adopted: February 17, 1997
Revised: August 23, 1999
Reviewed: March, 2002
Reviewed: March 2006