

# Merkel ISD

## Acceptable Use of Technology and Internet Safety Policy

*For Merkel High School and Middle School Students*

---

---

The technology resources MISD provides to students are intended to facilitate legitimate educational activities of the schools. The purpose of this policy is to insure that the district's technology resources are used only for appropriate purposes. In addition, this policy addresses preventing minors from accessing inappropriate material on the Internet, and the safety and security of minors. To gain access to the network and Internet, all students must obtain parental permission as verified by the signatures on the form attached to this policy.

The following rules apply to all technology-based equipment at Merkel High School and Middle School, including computer labs, classroom computers, telecommunications and AV equipment.

### **Acceptable uses of technology:**

***School computers are the property of MISD, and are for school-related use only.*** Acceptable activities include instruction, independent study, authored research, and the business of student organizations and activities. Examples of unacceptable uses include, but are not limited to:

- *Computers may not be used to harass or defame others.* This includes intentionally harming another's reputation, sending offensive or unwelcome messages, or making another person feel uncomfortable.
- *Any use of computers that violates the law or encourages others to violate the law is prohibited.* Examples include but are not limited to:
  - Selling or advertising any illegal substance
  - Downloading, viewing or transmitting pornographic images
  - Downloading, viewing or transmitting information on making weapons, planning violent events, or harming others.
  - Obtaining or transmitting confidential, trade secret information, or copyrighted materials.
- *Making copies of school software is prohibited.* In some cases, computers and software may be checked out and used at home. Your technology teacher or campus technology representative can assist you with this. All software installed on school computers must be approved by MISD technology director. Only licensed, approved software may be installed.
- *Do not download or install games, music, or other programs on school computers.* All games must be requested by teachers and used for instructional purposes only. File sharing programs such as Kazaa or LimeWire should not be used. Do not use school computers to load iPods or other MP3 players, except as directed by a teacher.
- *Any file sharing, other than what has been setup by MISD Technology department, is prohibited.* Do not configure computers to share files, and do not set up unauthorized networks within the district. Also, do not participate in peer-to-peer file-sharing networks.

- *Any form of vandalism of technology resources is prohibited.* This includes:
  - Uploading, developing or possessing a worm, virus, or other harmful programming
  - Participating in hacking or unauthorized access to networks or computers, including keystroke capturing and other methods designed to obtain passwords or computer access.
  - Altering or destroying data belonging to someone else
- *Do not use school resources, including mail and web servers, for commercial or political applications.*
- *Do not engage in activities that compromise the security of network access, other people's accounts, or other networks,* such as disclosing or sharing passwords with others; attempting to obtain passwords to bypass filters and routers, impersonating another user; using one's own software programs on the district's computers; altering computer settings; damaging or modifying computer equipment or software.
- ***Students should not be unsupervised while using computers.*** Any computer use by students must be monitored by a teacher or aide in the same room. ***Students should not be sent to computer labs without supervision.*** Enforcement of this policy requires that teachers and staff monitor students' use of the Internet to ensure compliance.
- *Do not change setting on computers,* including desktop backgrounds, control panel items, power settings, screensavers, etc. These may affect performance and compromise network security.
- *Each summer, all personal files on the servers will be deleted.* If you wish to keep these files, please copy them to a CD or jump drive and take them home.
- *Do not abuse or damage the computers or accessories.* Computers and accessories, such as headphones, cords, speakers, mice, etc., are school property. Any student who damages or destroys school property will be punished according to the guidelines in the MISD Student Code of Conduct, including the assessment of fines and/or cost of replacement. Repeated physical misuse of equipment could result in the loss of computer privileges.
- *Do NOT access social networking sites from school.* This includes MySpace, Facebook, Twitter, and similar sites.

## **Privacy**

***There is no expectation of privacy on school networks.*** Although it does not normally do so, the district reserves the right to access and monitor data storage areas, e-mail and Internet use. This information may be reviewed at random to insure compliance with district policy.

***Use your own user account only.*** Do not login as someone else. Put a password on your account to protect yourself.

- When logged on to your network account, you will have access to a personal data area (H: drive). Other students cannot see this data.
- You are responsible for your own userid and password. If you do not assign a password, or if you tell others what it is, you are still responsible for activities carried out using your userid.
- Accessing and using someone else's personal data area is prohibited.

- Personal data is limited to 75Mb. If you need more storage, please see your tech teacher.
- **Do not store music, games, or copyrighted information on your H drive.** Any such content found on your h-drive without notification.

## Plagiarism

*When using information obtained from the Internet or other electronic media, cite references for any facts you present.* Using copyrighted information without proper references is illegal. Users should assume that all materials are protected unless there is explicit permission on the materials to use them.

## Internet Safety

**Direct communication:** In order to avoid compromising the safety and security of minors when using e-mail, chat rooms, and other forms of direct electronic communications :

- *E-mail accounts not assigned by MISD are not permitted.* HotMail, Yahoo mail and similar public e-mail accounts are not to be accessed at school. **If your teacher sets up a Gaggle.Net e-mail account, you MAY use it at school.**
- *Real-time chat and instant messaging of any kind is prohibited.* Do not install IRC, IM, MSN, AIM, mySpace or other chat clients.

**Internet Filtering Technology:** Access beyond MISD's own network, specifically to the Internet and the World Wide Web, provides many opportunities for research and educational use. However, it raises safety concerns also. The safety and privacy rules that govern general technology and district computer use apply to the Internet as well. In addition, MISD employs technology protection measures that block or filter Internet access to some Internet sites that are not in accordance with the policy of MISD.

- The technology protection measure (filter) that blocks or filters Internet access may be disabled by a MISD staff member for bona fide research purposes **by an adult.** Students may NOT disable the filter.
- A staff member may override the technology protection measure that blocks or filters Internet access for a student to access a site with legitimate educational value that is wrongly blocked by the technology protection measure that blocks or filters Internet access.
- The filter password, if available, should NOT be given to students. If a student requires a staff member to override the block, the password must be entered by the staff member, and the staff member must remain to monitor the student's computer use.

- Students who attempt to override the filter may be disciplined. This includes, but is not limited to, using a password or proxy site to bypass the filter.
- MISD staff must monitor students' use of the Internet to ensure enforcement of policy. Students should not have access to the Internet without supervision.
- Users should be aware that filtering software does not block ALL inappropriate Web sites. Report all inappropriate sites not blocked by filters to a technology administrator for appropriate action.

***General Internet Safety:***

- Students shall not disclose personal information, such as name, school, address, phone numbers, etc. outside of the school network.
- Never arrange a face-to-face meeting with someone one has "met" on the computer network or Internet without a parent's permission.
- Any form of "cyberbullying" will not be permitted.
- Students involved in Web Development classes may post content to a MISD web server. When posting information, please take care not to violate the privacy of others, or jeopardize the health and safety of students. Do not post personal information, or use names with student pictures. In addition, avoid information which is obscene or libelous, causes disruption of school activities, or violates any other aspect of school policy.

*More information on how to use your network account is available from technology teachers or on the MISD web site. If questions arise concerning any part of this policy, please contact school administration for clarification.*

---

## **PARENT PERMISSION FORM and USER AGREEMENT – 2009-10**

As a parent or guardian of a student at MISD, I have read the above information about the appropriate use of computers at school and I understand this agreement will be kept on file at the school. (Questions should be directed to the principal for clarification). Please check one:

My child may use the MISD network and Internet while at school according to the rules outlined in the Acceptable Use of Technology Policy

I would prefer that my child not use the network and Internet while at school.

**Parent Signature** \_\_\_\_\_

**Parent Name (print)** \_\_\_\_\_

**DATE:** \_\_\_\_\_

---

---

## **PARENTS' PERMISSION FOR THE PUBLICATION OF STUDENT WORK/PICTURES**

I understand that from time-to-time the school may wish to publish examples of student projects, photographs of students, and other work on an Internet accessible web server. In these cases, the student will NOT be identified by name. Please check one:

My child's work can be published on the Internet and photographs of my child can be published

I would prefer that my child's work and picture not be published on the Internet \_\_\_\_\_

**Parent Name (print)** \_\_\_\_\_

**Parent Signature** \_\_\_\_\_

**DATE:** \_\_\_\_\_

---

---

As a user of the School computer network, I agree to comply with the above stated rules and to use the network in a constructive manner.

**Student Name (print)** \_\_\_\_\_

**Student Signature** \_\_\_\_\_

**DATE:** \_\_\_\_\_