

# Merkel ISD

## Acceptable Use of Technology and Internet Safety Policy

*For MISD Faculty and Staff*

---

---

The technology resources MISD provides to faculty and staff 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.

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

### ***Privacy:***

***There is no expectation of privacy on school networks.*** District computers and computer systems are owned by the district and are intended for educational purposes and district business at all times. Staff members shall have no expectation of privacy when using the Internet or electronic communications. All communications and information received via MISD technology systems is the property of the district.

The district and its telecommunication providers have the ability to monitor and store all Internet traffic. Although it does not normally do so, the district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all technology use. This information may be reviewed at random to insure compliance with district policy.

### ***Filtering and blocking obscene, pornographic and harmful information:***

To protect students from material and information that is obscene, pornographic, or otherwise harmful to minors, technology that blocks or filters such material and information has been installed on all district computers having Internet or electronic communications access.

- 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.
- 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, and staff should NOT allow students to override a block. If a student requires a staff member to override the block, the password must be entered by the staff member, who must then monitor the student's computer use. With the research databases available, it should not be necessary to bypass the filter for normal schoolwork.

- Any student or staff member who attempts to override the filter by any means, for activities other than bona fide research by an adult, may be disciplined. This includes, but is not limited to, using a password or proxy site to bypass the filter.
- **Students cannot be left 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.**
- Users should be aware that filtering software does not block ALL inappropriate Web sites. Report all inappropriate sites not blocked by filters to the technology coordinator for appropriate action.

### ***Unauthorized use of technology:***

**School computers are the property of MISD, and are for school-related use only.**

Personal components may not be added to district equipment. Computers and technology equipment are considered tools, not toys or babysitters. It is vital that students learn to use computers and Internet as part of their technology instruction. 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.* All games must be requested by teachers and used for instructional purposes only. File sharing programs such as Kazaa or Morpheus should not be used, and school computers should not be used to load iPods or other mp3 players. **This includes WeatherBug, WebShots,** and other 'harmless' programs, which can have a negative effect on network performance. **IF you need additional programs installed,** please check with technology first to ensure compatibility with networks and workstation.

- *Computers should not be used as babysitters.* If structured instruction is not available for any reason, students should not be sent to labs to play games or surf the Internet. An assignment should be provided and supervised. Students are not permitted to play games outside of structured instruction.
- *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. If you need some additional form of file-sharing for educational use, please contact the technology department.
- *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 other 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.* This includes sending political/campaign mail.
- *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.
- *Do not change settings on computers,* including adding desktop backgrounds, control panel items, power settings, screensavers, etc. These may affect performance and compromise network security.
- ***Teachers and staff members should NOT ask students to install software, repair computers, or answer technology questions.*** If a computer is not performing acceptably, contact the technology representative on your campus to have it repaired. If the problem is more extensive, he or she will contact the technology department for assistance. Student *staff members* may install authorized software at the request of staff, but **other students are not permitted to install ANY software.** Separate computers, not connected to the district's network, are provided for technical classes to use. Tech teachers may use these at their discretion.
- *Do not store digital camera images, video, or movies permanently on computer or network disks.* If you use your computer to download pictures from a digital camera, please edit, print, or copy the pictures you need, and delete the rest. The pictures can be easily copied to CD or DVD. Personal pictures should not be kept on MISD equipment and may be deleted without notice.
- *Do not abuse or damage the computers or accessories.* Computers and accessories, such as headphones, cords, speakers, mice, etc., are school property. Damage to school property may result in 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.
- Public blog and wiki sites *MAY* be used for legitimate educational purposes, provided they are not blocked by the filter. Podcasting is also permitted for educational use.

### **Security:**

Security on computer systems is a high priority. Anyone identifying a security risk should contact the network administrator immediately. Do not demonstrate the problem to others.

**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). Others 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 100Mb. If you need more storage, please consult the network administrator.
- Do not store music, games, or copyrighted information on your H drive.
- Do not attempt to gain access to systems as 'administrator' or 'sysop'

**Computers are monitored to evaluate performance and prevent problems.** Many computer settings can affect the system's vulnerability to viruses or other malicious attacks. MISD reserves the right to access all computers, either manually or through automated processes, to ensure that all security settings are current and optimal. Applications, programs or settings that potentially compromise security or impede computer management may be changed or removed

- Do not change settings on your computer
- Do not download and install programs from the Internet or from home without prior approval from the network administrator
- Do not disable virus protection on any computer

**Do not connect non-MISD computers or components to any part of the network.** Use of personal equipment on the network is prohibited. Consultants, presenters, and co-op employees may connect to the network **if the following criteria is met:**

- Current, non-web-based virus protection must be installed and enabled
- Windows computers must have all security updates applied

**It is the responsibility of campus administration to see that all invited presenters or consultants meet these requirements.** Call Technology for assistance if required.

**Do NOT give your password to substitute teachers.** Substitute teachers do **NOT** have computer privileges. Subs will take attendance on paper. If you need to make arrangements for a particular lesson plan, or a long-term substitute, please contact the technology department.

**Confidentiality:**

*Do not use the district's networks to transmit information protected by confidentially laws.* If information is sensitive but not legally protected, great care must be taken to ensure that only those with a 'need to know' can access the information. District technology personnel can assist in protecting information if necessary. Since Internet e-mail is an insecure and unencrypted transmission medium, avoid using it across the Internet for sensitive material.

**E-mail:**

A professional-quality e-mail account is provided to each district staff member. This account should be used for all district and campus business and communications. All staff members are expected to check their accounts regularly for district communications. **Do not use personal accounts for school business.**

This account is also accessible from home (or anywhere there is an Internet connection) and may be used off-campus if convenient. **Other personal e-mail accounts should NOT be used for school communications.** The signature page of this policy agreement must be received prior to having your e-mail account setup.

- Due to security concerns, **HotMail, Yahoo mail and similar non-standard public e-mail accounts are prohibited at school.** You can set up Gagle.net accounts for your student if required. Gagle is available at school or home.
- A limited amount of personal business may be conducted using your district account. Please remember that all accounts are property of the district and subject to review at any time. If personal e-mail becomes excessive, your e-mail account may be revoked.
- Do not propagate urban legends, chain letters, or other unnecessary e-mail using your school account.
- Do not send mass-mailing virus alerts without approval of the network administrator. Most of these are hoaxes. If you send other mass-mailed information to campus or district accounts, please make sure it is of educational value and applies to all concerned. The subject line should be descriptive, and the mail content as concise as possible. Information that applies to the workplace may be posted – the following mass e-mail announcements would be permitted:
  - Campus or district sponsored events
  - Official policy changes

- Messages regarding disruptions of services (power or phone outage, etc)
- Government-related messages
  
- MISD filtering technology attempts to limit the amount of unsolicited junk mail (spam) received by district employees, without hindering legitimate e-mail. However, we cannot protect users from receiving all mail offensive to them. If you receive offensive e-mail, please trash it or use the 'junk mail' features of the e-mail system to deal with it. If you feel that you are receiving excessive spam (>10-15 e-mails per day), or if the system is blocking your legitimate mail, please contact the system administrator.
  
- Students do not normally have MISD-issued accounts. If they require e-mail for a school project, free student-safe e-mail is available from guggle.net. Teachers can set up and monitor student accounts as necessary. If you need assistance, please contact the system administrator.
  
- E-mail in teacher accounts will only be held 9 months. If you need to keep e-mail longer than 8 months, please print or archive it using the GroupWise client.
  
- MISD does not currently archive staff e-mail. Deleted mail is not available once the individual 'trash' folders have been purged.

## **Internet Safety**

### ***Instant Messaging or Chat:***

- Due to security risks, **do not install or use Instant Message clients such as MSN, AIM, mySpace or Yahoo chat.**
- The GroupWise Messenger program is installed on each teacher computer. This 'instant message' program facilitates staff communication by allowing teachers & staff within the district to communicate quickly with each other. Other chat programs are not permitted. For more information on using GroupWise Messenger, see R:\Teacher Info\GroupWise Messenger.

### ***General Internet Safety:***

**Internal Web Server:** Students in Web Development or other classes may post information to an internal MISD web server, which is accessible via the Internet. Teachers involved in such projects must ensure that the students understand the rules of safe posting:

- Take care not to violate the privacy of others, or jeopardize the health and safety of students.
- Do not post personal information,

- Do not use student photos or artwork without parental permission.
- Never post a student's name with photo or artwork.
- Avoid information which is obscene or libelous, causes disruption of school activities, or violates any other aspect of school policy.

**Faculty/Staff Web Pages:** A managed content web server is maintained by Region XIV for MISD faculty and staff to post Internet content. The district encourages each staff member to develop their web pages as a method of communication between student, parents, and staff. Instructions on how to access your web account are available through your campus technical representative or network administrator. The rules safe posting, as listed above, also apply to teacher web pages. In addition:

- Take care not to publicize the times, dates and locations of events such as field trips. This information could be used by non-custodial parents and others wishing to locate a child.
- Be aware of social services rules, especially concerning photographs and publicity of children in protective custody.

- **Other**

- Do not disclose personal information, such as name, school, address, phone numbers, etc. outside of the school network.
- Never arrange a face-to-face meeting, or allow a student to meet with someone one has "met" on the computer network or Internet

---

---

*Detailed information on how to use your network and e-mail accounts is available from technology teachers or on the school web site. If questions arise concerning any part of this policy, please contact school administration for clarification.*

---

---

This page intentionally left blank

**FACULTY USER AGREEMENT – 2009-10**

As a member of faculty or staff at MISD, I have read the above information regarding the appropriate use of computers at school. I understand this agreement will be kept on file at the MISD. (Questions should be directed to the technology director or assistant superintendent for clarification).

I agree to abide by all district policies, including this Acceptable Use Policy, and other district publications that address technology-related issues. I further agree to comply with directives regarding revisions and clarification of these policies, from district officials acting in performance of their duties.

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

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

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

---

---

As a user of the district e-mail account, I agree to comply with the above stated rules regarding the district's e-mail policies:

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

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

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