

AISD ACCEPTABLE USE POLICY

The following are “paraphrased highlights” of the AISD Student Code of Conduct – the original full, legal text is located on pgs. 41 – 43 of the handbook.

The following information is provided so that **students, parents and staff** are aware of **responsibilities** involved in the efficient, **ethical** and **legal use** of technology resources. (Collectively referred to as the electronic communications system – referred to here, within, as “the system”)

Students will be required to adhere to all District policies and to Internet Safety and Acceptable Use Guidelines.

- Access to the District’s electronic communications system is a **privilege**, not a **right**.
- Access to the system is available to students for instructional and administrative purposes only.

Noncompliance may result in

- suspension of access
- termination of privileges
- disciplinary action consistent with District policies.

CONSENT REQUIREMENTS

1. Only specifically authorized persons may load software to the system.
2. Student work will not be posted on a web page without written consent from the student (and the student’s parents, if the student is a minor).
3. No personally identifiable information about a student will be posted on a web page without written consent from the student’s parent.

FILTERING

1. Internet access will be filtered.
2. In appropriate material will be blocked. Categories will include, but not be limited to:
 - nudity/pornography;
 - images or descriptions of sexual acts
 - promotion of violence
 - drug uses
 - discrimination, or participation in hate group
 - illegal use of weapons
 - instructions for performing criminal acts (e.g., bomb making)\online gambling

SYSTEM ACCESS

1. Students will be given individual accounts and granted access to the system as appropriate.
2. Students identified as a security risk or as having violated guidelines may be denied access to the system.
3. All users will be required to sign a user agreement annually.

INDIVIDUAL USER RESPONSIBILITIES

1. Each student will be responsible at all times for the proper use of his/her account.
2. If students know about a security problem they should report it to a teacher without revealing the information to other students.
3. Students may not:
 - disable, or attempt to disable, a filtering device
 - encrypt communications

- use another person’s account
- give out personal info via the system – i.e. address & phone #
- use the network for financial/commercial gain, advertising or political issues
- **use personal email or chat features/rooms while on district systems**
- share copyrighted software with others
- **waste system resources – i.e. playing videos, etc without permission**
- gain unauthorized access to resources or information
- purposefully access, use, send/post materials that are:
 - pornographic
 - threatening, harassing
 - sexually oriented
 - damaging to another’s reputation
 - obscene
 - illegal
 - abusive

VANDALISM

- Any malicious attempt to harm or destroy equipment or data is prohibited.
- Deliberate attempts to degrade/disrupt system performance may constitute criminal activity under applicable state and federal laws. (i.e. uploading viruses)
- Vandalism will result in
 - cancellation of system use privileges
 - restitution for costs associated
 - other appropriate consequences.

FORGERY PROHIBITED

The following is prohibited:

- Forgery or attempted forgery of e-mail messages is prohibited.
- Attempts to read, delete, copy or modify the e-mail of others
- deliberate interference with others attempts to send/receive electronic mail
- use of another person’s user ID and/or password

INFORMATION CONTENT/THIRD-PARTY SUPPLIED INFORMATION

- Students and parents should be aware that, despite the District’s use of technology protection measures, access to other resources within the global electronic network containing inaccurate and/or objectionable material might occur.
- A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.
- A student knowingly bringing prohibited materials into the system will be subject to”
 - suspension of access
 - revocation of privileges to the system
 - subject to disciplinary action in accordance with the Student Code of Conduct.

NETWORK ETIQUETTE

1. Be polite; messages typed in capital letters are equivalent to shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Transmitting obscene messages or pictures is prohibited.
4. Using the network in such a way that would disrupt the use by others is prohibited.

TERMINATION/REVOCATION OF SYSTEM USER ACCOUNT

Termination of a student's access for violation of District policies will be effective on the date the principal or District administrator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

MHS Student Code of Conduct (pages 63-64)

USE OF COMPUTERS

Use of MHS computers and network system & access to the Internet is a privilege, not a right. Uses which might be acceptable on a user's private personal account or system may not be acceptable on the MHS systems.

LESSER INFRACTIONS

- **Placing food/drink, make-up, liquids near the computer**
- Turning computer on/off w/out permission
- Keying in language which is inappropriate
- Changing display settings in anyway
- Keying in language which is inappropriate (see full text for specifics)
- Intentionally interfering w/another student's ability to do his work
- **Accessing games without permission**

POSSIBLE CONSEQUENCES FROM REFERRAL

- 7 lunch detentions + assistant principal will call parent
- 4 days OCS with parent call
- Removal from the class; may result in loss of credit.

SEVERE INFRACTIONS (see full text for complete list)

- **Bringing in outside storage devices**
- Modifying any software
- Loading or using unauthorized software
- Vandalism (such as stealing memory or computer accessories, sticking a pencil in the fan, switching voltage)
- Intentionally trespassing in files which belong to others
- Violation of copyright laws
- Accessing websites not related to the assignment
- **Accessing or distributing personal e-mail, instant messaging**
- Purchasing goods or services

CONSEQUENCES

- 4 days of OCS with parent call
- Assignment to Alternative Educational Program (CHOICES)
- Removal from class; may result in loss of credit

Typically, a student will not be assigned On-Campus Suspension and/or be suspended more than three times. Consequences for any additional referrals will be determined at a Principal level hearing.

This is a partial list of infractions and accompanying consequences to be used as a guide in making good decisions. It is not meant to be a complete list. If you have questions concerning any area not covered in this document, please contact your assistant principal for clarification.