Mt. Enterprise ISD

Electronic Communications System & Internet Safety Policy

Approved by MEISD Board of Trustees 6/11/2012

Section 1: Administrative Policies

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

Availability of Access

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;

2. Does not unduly burden the District's computer or network resources; and

3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Access to the District's electronic communications system will be governed as follows:

1. As appropriate and with the approval of the immediate supervisor, District employees will be granted access to the District's system.

2. Students in grades K-12 will be granted access to the District's system by their teachers, as appropriate.

3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.

4. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Monitored Use

Electronic mail transmissions and other use of the electronic communications system by students (minors) and employees are not private and may be monitored at any time by designated District staff to ensure appropriate use.

It shall be the responsibility of all members of Mt. Enterprise ISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Internet Filtering

Internet filtering software is provided as a condition of the Internet access service agreement that Mt. Enterprise I.S.D. currently holds with Region VII E.S.C. (esc7net). If this provision is removed or discontinued from said agreement, Mt. Enterprise I.S.D. will provide appropriate filtering software at the district level. Content filtered will include, but is not limited to, visual depictions deemed obscene, child pornography, and content harmful to minors.

In accordance with the CIPA and subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Student Training/Education

Mt. Enterprise ISD or its designated representatives will provide age-appropriate training for students who use the district's Internet facilities. The training provided will be designed to promote Mt. Enterprise ISD's commitment to:

> a. The standards and acceptable use of Internet services as set forth in the MEISD's Internet Safety Policy;
> b. Student safety with regard to:
>> i. safety on the Internet;
>> ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
>> iii. cyberbullying awareness and response.
> c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Intellectual Property Rights

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created for its use by an employee even when the author is no longer an employee of the District.

Email Archival

Mt. Enterprise ISD shall subscribe to email archival service provided by ESC7net. Any email retrieval will be requested by MEISD and performed by employees of ESC7net.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

Personal Internet-Connected Devices

Use of personal devices while on school or district property is subject to the provisions in the District Electronic Communications System & Internet Safety Policy. Unauthorized and/or inappropriate access to district network resources is prohibited. Access to or exchange of inappropriate materials is also prohibited while on district property.

Section 2: Acceptable Use Policy

The Mt. Enterprise Independent School District recognizes that computers and other electronic information/communications systems are used to support learning and to enhance instruction. Computer information networks allow people to interact with many other computers and networks. It is a general policy that all computers are to be used in a responsible, efficient, ethical, and legal manner.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

The following standards will apply to all users of the District's electronic information/communications systems:

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work.

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act and District policy.

On-Line Conduct

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.

4. Students may not distribute personal information about themselves or others by means of the electronic communication system.

5. System users must purge electronic mail in accordance with established retention guidelines.

6. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

7. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may noncommercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.

11. System users may not waste District resources related to the electronic communications system.

12. System users may not gain unauthorized access to resources or information.

13. System users may not intentionally disrupt information network traffic or crash the network and connected systems.

14. System users may not use the system for commercial or financial gain or fraud.

15. System users may not post anonymous messages.

16. System users may not possess any data which might be considered a violation of these rules in paper, magnetic (disk), or any other form.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

Information Content / Third Party Supplied Information

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

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 school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

Participation in Chat Rooms and Newsgroups

Students are prohibited from participating in any chat room or newsgroup accessed on the Internet. Such participation is permissible for employees, in accordance with District policies.

Development of Web Pages

The Technology Coordinator and any assistant(s) he deems necessary will be responsible for the maintenance of the district's web site. The district's web site resides at the URL http://www.meisd.esc7.net . The district will not be responsible for any other web sites which have any reference to or claim of ownership by Mt. Enterprise I.S.D.

Network Etiquette (Netiquette)

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.

2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

3. Pretending to be someone else when sending/receiving messages is considered inappropriate.

4. Transmitting obscene messages or pictures is prohibited.

5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Consequences of Acceptable Use Policy Violations

Consequences of violations may include but are not limited to the following:

1. Suspension of access to any or all components of electronic information/communications system
2. Revocation of access to any or all components of electronic information/communications system
3. ISS (Students only)
4. AEP (Students only)

5. School Expulsion (Students only)
6. Legal action and prosecution by authorities

Termination / Revocation of System User Account Disclaimer

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

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.